Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Risk Informed Resource Allocation at the Department of Homeland Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**10**	

TESTIMONY

Risk Informed Resource Allocation at the Department of Homeland Security

HENRY H. WILLIS

CT-272

February 2007

Testimony presented before the House Appropriations Committee, Subcommittee on Homeland Security on February 7, 2007

Published 2007 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
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. Willis[1]
The RAND Corporation

Risk-Informed Resource Allocation at the Department of Homeland Security

Before the Committee on Appropriations
Subcommittee on Homeland Security
United States House of Representatives

February 7, 2007

Mr. Chairman and distinguished members of the subcommittee, thank you for the opportunity to speak today about the task of allocating resources to protect the United States from terrorism.

Many of my comments are based directly on RAND Corporation research on the topics of estimating terrorism risk and allocating resources to manage these risks. Much of this work was made possible through RAND's program of self-initiated research—funded through the independent research and development provisions of our Federally Funded Research and Development Centers—and through grants to RAND from the Department of Homeland Security (DHS) Homeland Security Centers of Excellence programs.

My testimony is built around four key observations from our work on risk-informed resource allocation:

- There is no single correct method for measuring terrorism risk.
- Homeland security expenditures should be held to the same standard of effectiveness as expenditures for other government functions.
- Congress should hold DHS accountable to continuing the adoption of a capabilities-based planning approach to homeland security.
- Congress should provide clear direction and resources to DHS so that the Department will have the capacity to conduct analysis of cross-agency risk management and strategic planning issues.

Whatever approach Congress chooses to adopt in the allocation of investments in homeland security, it must ultimately decide how to balance two objectives: allocating federal resources to make the nation as a whole a safer place, or allocating resources to achieve equity among states

[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.

and localities. Sometimes these objectives will be at odds with each other. A lack of clarity and transparency into how these objectives are balanced will undermine the credibility of the Federal homeland security enterprise.

Context

Since the formation of DHS in 2003, Congress and DHS have made continuing progress in incorporating risk analysis into decisionmaking about homeland security policy and programs. For example, 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 was intended to serve as a surrogate measure of the consequences of terrorist events. 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, Secretary Michael Chertoff has called on DHS to adopt risk-based decisionmaking. The principle of using risk-based decisionmaking has now been adopted across DHS and methods of risk analysis are becoming established in DHS.

Terrorism risk is a function of three factors: a credible *threat* of attack on a *vulnerable* target that would result in unwanted *consequences*. Risk only exists if terrorists want to launch an attack, if they have the capability to do so successfully in a way that avoids security and compromises the target, and if the attack results in casualties, economic loss, or another form of unwanted consequence.

Models to estimate terrorism risks and the outcomes of terrorist attacks under various scenarios have been developed at DHS Centers of Excellence, independent think tanks, other research organizations, national laboratories, and the Department of Defense. DHS itself has also developed models and sponsored external research, including a RAND study on the using risk analysis for intelligence analysis sponsored by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). Risk management and the tools to support it are being institutionalized into the DHS decisionmaking process.

The National Infrastructure Protection Plan (NIPP), released last year, reflects one example of this institutionalization by defining comprehensive approach to risk assessment across economic sectors. Compared to earlier drafts of this document, the final NIPP reflects Secretary Chertoff's guidance to use risk-based decisionmaking and represents the advanced state of DHS thinking on critical infrastructure protection. Specifically, it takes a balanced approach to incorporate risk assessment; information sharing, feedback, and training; organizing and partnership with private

sector; resource allocation; and long-range sustainability of protection efforts. Finally, the NIPP describes a framework that follows the best practices of risk analysis that are outlined in, among other places, the National Research Council in its foundational reports *Risk Assessment in the Federal Government: Managing the Process* (1983) and *Science and Judgment in Risk Assessment* (1994). These best practices require that risk assessments be: (a) analytic, (b) deliberative, and (c) practical. For homeland security policy, these statements have the following translation:

a. Analytic

An analytic process must address all three factors that determine terrorism risk— threat, vulnerability, and consequences—and, where feasible, do so quantitatively. Risk assessments must be repeatable so all parties can replicate, analyze, and understand them. Over the past three decades, the Environmental Protection Agency has developed analytic methods of risk analysis to decide when a Superfund site is clean, and the Nuclear Regulatory Commission has developed them to decide when a nuclear power plant is safe. Many of these analytic techniques are now being applied to the study of terrorism. However, the uncertainty inherent in terrorism risk, particularly in the terrorist threat, implies that, unlike most of our successful experience with risk analysis tools in the past, some new thinking about all plausible threats, not just the most likely threat, will also need to be taken into account.

b. Deliberative

A deliberative process is necessary because the notion of a cold, actuarial terrorism risk assessment is unrealistic. Values and judgment are part and parcel of the process and require transparency and a comprehensive public discussion of outcomes. For example, consider whether more should be spent to protect a skyscraper in downtown Los Angeles from damage from terrorism or from earthquakes, or whether more should be spent on this skyscraper or the buildings in the Los Angeles School district. Public discourse is the only way to address credibly 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.

c. Practical

Finally, risk assessment must be practical, which means that data collection and management requirements must be technically and economically feasible. Further, estimates should not overly rely on a single perspective or tool. In these aspects significant challenges still remain in implementing risk assessment at DHS but these concerns relate more to implementing what is called for in policy documents like the NIPP than to concerns with the concepts such documents outline. For example, there are more than 10,000 hazardous chemical facilities across the United

States, and these represent only one of the critical infrastructures mentioned in the NIPP. How practical is it to conduct risk analyses of the entire chemical sector given limitations in funding, time, and staff available? These issues have not been fully ironed out and the scale of this problem may make assessing risks to critical infrastructure infeasible if methods are not adjusted appropriately. Adding to the complexity, implementation will need to address both natural disasters and terrorist threat.

Observations

With this as background, there are four observations from our work that are pertinent to today's hearing.

First, there is no single correct method for measuring terrorism risk. Risk management is currently the responsibility of the many entities in DHS—it is not owned by any one part of DHS. Each approach used by the various entities has its own strengths and shortcomings. Also, different purposes require different analyses appropriate to the task.

It is important to differentiate between strategic risk assessment and risk assessment to support tactical or operational decisions. Strategic assessments might guide the distribution of resources that are not reallocated frequently, such as the state, port, and urban area grants that DHS administers. Tactical and operational assessments might be in response to intelligence about specific threats (actionable intelligence) or events that have already occurred. These distinctions also vary at different levels of government.

Of course, all such assessments are needed, but the role of the Federal government may be different in each case. For strategic risk assessments, it is necessary and appropriate to have Federal leadership. The goal is to distribute resources in roughly the right place and correct proportion so that corresponding local and state authorities can use those resources appropriately. RAND analysis of the Urban Area Security Initiative demonstrates how risk analysis can be used in this context[2].

Then again, if the risk assessment is intended to direct tactical decisions, such as expenditures to protect a specific facility or position law enforcement in response to a specific threat, then the state and local authorities may need to play a larger role in risk assessment and resource

[2] Willis, H. H., A. R. Morral, T. K. Kelly, J. J. Medby (2005). *Estimating Terrorism Risk.* MG-388-RC, RAND Corporation, Santa Monica, CA. Online at http://www.rand.org/pubs/monographs/MG388 as of February 1, 2007.

allocation decisions. An example of this would be planning for security around points of distribution for the Center for Disease Control's Strategic National Stockpile Assets.

Second, homeland security expenditures should be held to the same standard of effectiveness as expenditures for other government functions. Ultimately, the goal of homeland security regulation, grant programs, and activities should be to reduce most effectively the risks of terrorism and natural disasters. Analyzing homeland security programs using metrics such as residual risk (i.e., the risk remaining after a regulation or program is implemented) or cost effectiveness (i.e., dollars per life saved or dollars per dollar of economic activity preserved) allows these expenditures to be compared to each other, as well as compared to expenditures directed toward other goals like national security, healthcare, the environment, or education.

The first step in this process is implementing periodic, independent assessments to evaluate how homeland security efforts have succeeded in reducing risk. These assessments will enable a feedback mechanism that can ultimately help make risk reductions more effective. Such assessments would benefit the DHS grant programs, as well as border and maritime security programs like the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), the Customs-Trade Partnership Against Terrorism (C-TPAT), the Maritime Transportation Security Act (MTSA), and the Transportation Security Administration's baggage and passenger screening and profiling programs. RAND assessments of screening shipping containers at maritime ports[3] and security enhancements at Los Angeles International Airport[4] provide examples of how risk analysis can be incorporated into such evaluations.

In preliminary analysis by RAND of the Urban Area Security Initiative grant programs, it appears that at least some of the DHS programs are managing risks in a manner consistent with decisions made across other parts of the federal government, such as the Environmental Protection Agency, the Occupational Safety and Health Administration, and the Department of Transportation[5]. However, DHS must apply more thorough program evaluation and analysis of risk management expenditures.

---

[3] 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.

[4] Stevens, D., T. Hamilton, M. Schaffer, et al. (2006). *Implementing Security Improvement Options at Los Angeles International Airport*, DB-499-LAWA-1, RAND Corporation, Santa Monica, CA. Online at http://www.rand.org/pubs/documented_briefings/DB499-1 as of February 1, 2007.

[5] Willis, H. H. (2006). *Guiding Resource Allocations Based on Terrorism Risk*. WR-371, RAND Corporation, Santa Monica, CA. Online at http://www.rand.org/pubs/working_papers/2006/RAND_WR371.pdf as of February 1, 2007.

Third, Congress should hold DHS accountable to continuing the adoption of a capabilities-based planning approach to homeland security. My colleague at RAND Paul Davis defines capabilities-based planning as, "planning, under uncertainty, to provide capabilities suitable for a wide range of modern-day challenges and circumstances while working within an economic framework that necessitates choice."[6] This is a logical follow-on to using risk analysis to guide resource allocation decisionmaking. Uncertainties about when, where, and how the next terrorist attack or natural disaster will occur mean that is impossible and inappropriate to develop a risk management plan optimized for a narrow estimate of future threats. Rather, when planning for multiple missions and confronting deep uncertainty more effective decisions are made by adopting plans that are flexible, adaptive, and robust. Here *flexible* means plans can address new threats as they emerge; *adaptive* means plans are effective even if anticipated threats emerge in unanticipated ways; and *robust* means plans provide capability even in cases where a terrorist or natural disaster compromise a component of the planned defense or response. In responding to Homeland Security Presidential Directive 8 on National Preparedness, DHS has built the foundation for capabilities-based planning by defining National Planning Scenarios, a Universal Task List, and a Target Capabilities List to guide planning. Continued application of these tools to develop *flexible, adaptive and robust* strategies when considering all the Department's missions and all threats from both terrorism and natural disasters can improve risk management at DHS.

Finally, Congress should provide clear direction and resources to DHS so that the Department will have the capacity to conduct analysis of cross-agency risk management and strategic planning issues. Capabilities-based planning and analysis for homeland security as I have outlined requires multidisciplinary skills. Engineers and natural and physical scientists are needed to understand the consequences of weapons, pandemics, and natural disasters. Social scientists are necessary to understand how these events affect communities and how terrorism security efforts influence terrorists' intentions. And skilled public administrators are needed to shape the results of these analyses into effective policy and programs.

These capabilities must be available both inside and outside DHS. Internal institutions can provide DHS with a capability to digest external analysis, self-critique Department efforts, and, ultimately, improve the Department's programs. Trusted external institutions can provide independent perspectives on DHS progress in risk management.

---

[6] P. K. Davis (2002). *Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation.* MR-1513-OSD, RAND Corporation, Santa Monica, CA. Online at http://www.rand.org/pubs/monograph_reports/MR1513 as of February 1, 2007.

Internally, the foundation for capabilities-based planning and analysis already exists in many places in DHS, such as the Office of Program Analysis and Evaluation, the Office of the Assistant Secretary for Policy, and the Office of the Under Secretary for Management. There is a proposal for an Assistant Secretary-level office for risk analysis where much of this work could also be consolidated. With appropriate authority and resources, analysis shops in all these offices could support capabilities-based planning and analysis.

Externally, the Department can use work from the existing body of DHS Centers of Excellence, independent think tanks, other research organizations, and national laboratories. The Department could also be well served by creating a Federally Funded Research and Development Center to support the Office of the Secretary of Homeland Security by providing trusted, independent, and objective *policy* analysis. Though the Department currently does have a Federally Funded Research and Development Center, that Center supports the Under Secretary of Science and Technology, not the Secretary directly; as a result, that Center is more limited in its ability to study and influence Department-wide resource allocation and other strategic issues.

In closing, over the past year, much has been made about decisions to allocate resources to or away from particular localities around the country. In any risk-informed decision process constrained by limited resources—which is certainly the case here—tough choices must be made, and not every community will be happy with those choices all the time. Avoiding these choices by trying to satisfy all needs has serious consequences: resources may be spread too thinly such that no locality can provide sufficient capability to protect, mitigate or respond to terrorism effectively. However, if DHS adopts a reasoned, analytic, capabilities-based approach to resource allocation of the type outlined above—one that is open and transparent to stakeholders—the Department will instill more confidence in the public that they are doing their best to make the country a safer place.

Thank you again for the opportunity to address the subcommittee on this important subject, and I look forward to answering any questions you may have.