TESTIMONY

Analyzing Terrorism Risk

HENRY H. WILLIS

CT-265

July 2006

Written testimony submitted to the House Financial Services Committee, Subcommittee on Oversight and Investigations, and the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment on July 25, 2006

Published 2006 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

Statement of Henry H. Willis, Ph.D.[1]
The RAND Corporation

Analyzing Terrorism Risk

Before the Committee on Financial Services
Subcommittee on Oversight and Investigations
and
Before the Committee on Homeland Security
Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
United States House of Representatives

July 25, 2006

I would like to thank the distinguished Chair for the opportunity to present written testimony about terrorism risk assessment at the Department of Homeland Security (DHS). Many of my comments are based directly on a recently released RAND Corporation report entitled, "Estimating Terrorism Risk," which has been made available to Members of the Committee. This report is part of RAND's program of self-initiated research that is funded through the independent research and development provisions of our Federally Funded Research and Development Centers. It is a recent release by the RAND Center for Terrorism Risk Management Policy, which was established in 2002 to study terrorism risk management, insurance, liability, and compensation. I would like to request that this report be made part of the official record.

Over the last four years, Congress and the Department of Homeland Security have made tremendous progress in maturing homeland security policy. Shortly after September 11, 2001, decisions were dominated by the use of crude indicators, such as population, which approximated consequences of terrorist events. Subsequently, policy moved to vulnerability reduction and more recently, Secretary Michael Chertoff has called on the DHS to adopt risk-based decisionmaking. The next step in this process will be to focus on risk reduction and cost effectiveness, but the U.S. Government currently is in the early phases of moving in this direction.

The recently released National Infrastructure Protection Plan (NIPP) reflects this progression by defining an aggressive and comprehensive approach to risk assessment across sectors that

[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.

affect the U.S. economy. As compared to earlier drafts of this document, it reflects adoption of Secretary Chertoff's guidance to use risk-based decisionmaking and represents the state of the Department's thinking on critical infrastructure protection. Specifically, it tries to take 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 subsequently *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 requires addressing all three of the factors that determine terrorism risk: 1) threat, 2) vulnerability, and 3) consequence, and where feasible, to do so quantitatively. Risk assessments must be repeatable so all parties can replicate, analyze, and understand them. However, the uncertainty inherent in this problem, particularly in the terrorist threat, implies that unlike most of our successful experience with these tools in the past, some new thinking about all plausible threats, not just the most likely threat, will need to be taken into account.

b) Deliberative

A deliberative process is necessary because the notion of a cold, analytic risk assessment is a myth. Values and judgment are part and parcel to the process and require transparency and a comprehensive discussion of outcomes. This is the only way to credibly address tradeoffs between risks to people from risks to property and risks from a conventional bomb, nuclear attack, biological attack, or even hurricane or other natural disaster.

c) Practical

Finally, risk assessment must be practical, meaning that data collection and management requirements must not be untenable and estimates should not be overly reliant on a single perspective or tool. This last point is where concerns may arise with the draft NIPP. These concerns relate more to implementing what is outlined rather than concerns with the content of the plan itself. Implementation will need to address natural disasters as well as terrorist threat as the plan is used. Questions remain about the practicality of implementing risk analysis and

information sharing given limitations in the real world as to funding, time, and staff available. These issues have not been ironed out.

With this as background, there are 5 recommendations from our work that are pertinent to today's hearing.

First, the U.S. Government should consistently define terrorism risk in terms of metrics like expected annual consequences. Critical infrastructure risk assessment is too often focused on potential consequences, either ignoring or under emphasizing factors that determine threat and vulnerability. Expected annual consequences take threat, vulnerability and potential consequences into consideration in a rational way. Defining terrorism risk in terms of all of these factors facilitates the incorporation of risk reduction as the goal of homeland security programs.

Second, DHS should seek robust risk estimators that account for uncertainty about terrorism risk and variance in citizen values. Given the tremendous uncertainties surrounding terrorism risk assessment, it is prudent to plan for the range of plausible futures that may play out. Many different models exist and experts disagree on terrorists' capabilities and intentions. Risk assessment should reflect all credible models and expert judgments. The challenge is to support a single decision, while still being able to identify how risk is distributed differently across different outcomes, such as fatalities or property damage, and also explain how the decision would change if more emphasis were given to a single type of outcome or perspective on threats and vulnerabilities.

Third, DHS should use event-based models to assess terrorism risk. Measuring and tracking levels of terrorism risk is an important component of homeland security policy. These data provide insight into how current programs are reducing risk and when and where new terrorist threats may be emerging. Only event-based models of terrorism risk provide insight into how changes in assumptions or actual levels of threat, vulnerability, and consequences affect risk levels. There are many types of event-based models in existence. In our report, we relied on the Risk Management Systems (RMS) Terrorism Risk Model. This and other insurance industry models could also be used to support homeland security policy. The national laboratories have made progress on detailed models of critical infrastructures and their interdependencies. Colleagues in academia are applying economic input-output analysis to understand these same dependencies. Finally, the NIPP points to RAMCAP, or Risk Assessment Methodology for

Critical Asset Protection, which is based on a foundation for risk analysis consistent for methods used in reliability analysis and also with the National Research Council framework.

Fourth, relying on event-based models does not mean relying entirely on a top down process. It is important to differentiate strategic risk assessment from risk assessment to support design or performance assessment or that to support tactical decisions. Strategic assessments might guide the distribution of resources that are not reallocated frequently. Design and performance assessment might be used to optimize or tune a response to a particular threat or protect a specific asset. Think of assessment used to reinforce the design of a nuclear power plant. Tactical assessments might be in response to intelligence regarding specific threats (actionable intelligence) or events that have already occurred.

Of course all are needed. I recommend that a top-down approach is most practical for strategic risk assessment; and estimates need not be as detailed as design or tactical risk assessment. The goal is to distribute resources in roughly the right place and correct proportion. On the other hand, I recommend a bottom-up approach to support design or tactical decisions. Here more detailed models and analysis can be used to authorize spending on specific projects and justify current programs.

Strategic risk assessment ultimately needs event-based models. Until event-based models are more widely used to assess terrorism risk, density-weighted population is preferred over population as a simple risk indicator. Density-weighted population is simply a regions population multiplied by its population density. Our report found this metric to be reasonably correlated with the distribution of terrorism risk across the United States, as estimated by event-based models like the RMS Terrorism Risk Model. In contrast, our results suggest that population offers a remarkably weak indicator of risk, not much superior to estimating risk shares at random.

Finally, the U.S. Government should invest resources to bridge the gap between terrorism risk assessment and resource allocation policies that are cost effective. As I intimated earlier, Congress and DHS are only in the position to estimate risks and distribute resources where the risks are believed to be the largest. Ultimately, the goal should be to distribute those resources where they most effectively reduce risk. The first step in this process is implementing annual, independent risk impact assessments to evaluate how risk reduction funds have succeeded in reducing risk. These assessments will provide a feedback mechanism that will ultimately help increase reduction of risk. Such assessments would benefit the DHS grant

programs as well as border and maritime security programs like US-VISIT, C-TPAT, the MTSA, and TSA's baggage and passenger screening and profiling programs. The second step is a capabilities-based assessment of the nation's homeland security programs to document the unique contribution provided by each program and ensure appropriate balance to the layered defenses that have been put in place.

I would like to thank you again for the opportunity to address the committee on this important subject.