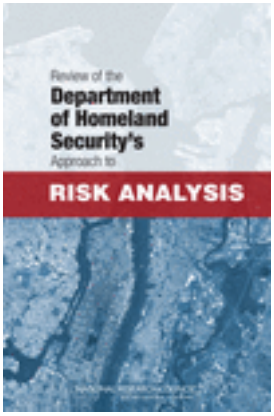

Review of the Department of Homeland Security's Approach to Risk Analysis

Committee to Review the Department of Homeland Security's Approach to Risk Analysis; National Research Council

ISBN: 0-309-15925-3, 160 pages, 6 x 9, (2010)

Review of the Department of Homeland Security's Approach to RISK ANALYSIS

Committee to Review the Department of Homeland Security's
Approach to Risk Analysis

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the Department of Homeland Security under sponsor award HSHQDC-08-C-00090. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. government.

International Standard Book Number—13: 978-0-309-15924-1
International Standard Book Number—10: 0-309-15924-5

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America.

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievement of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice-chair, respectively, of the National Research Council.

www.national-academies.org

Committee to Review the Department of Homeland Security's Approach to Risk Analysis

John F. Ahearne, Chair, Sigma Xi (Executive Director Emeritus), Research Triangle Park, North Carolina, and Duke University, Durham, North Carolina
Gregory B. Baecher, University of Maryland, College Park
Vicki M. Bier, University of Wisconsin, Madison[1]
Robin Cantor, Exponent, Inc., Alexandria, Virginia
Timothy Cohn, U.S. Geological Survey, Reston, Virginia
Debra Elkins, Allstate Insurance Company, Northbrook, Illinois[2]
Ernest R. Frazier, Sr., Countermeasures Assessment and Security Experts, Middletown, Delaware
Katherine Hall, BAE Systems, McLean, Virginia
Roger E. Kasperson, Clark University (Emeritus), Worcester, Massachusetts
Donald Prosnitz, Consultant, Walnut Creek, California
Joseph V. Rodricks, ENVIRON, Arlington, Virginia
Monica Schoch-Spana, University of Pittsburgh Medical Center, Baltimore, Maryland
Mitchell J. Small, Carnegie Mellon University, Pittsburgh, Pennsylvania
Ellis M. Stanley, Sr., Dewberry, Los Angeles, California

NRC Staff

Stephen D. Parker, Study Director
Scott T. Weidman, Deputy Study Director
Stephan A. Parker, Scholar Associate
Glenn E. Schweitzer, Scholar Associate
Ellen A. de Guzman, Research Associate
Stephen Russell, Senior Program Assistant

[1] Dr. Bier resigned from the committee on July 1, 2009, when she began to perform research supported by the Department of Homeland Security (DHS).
[2] Dr. Elkins resigned from the committee on December 7, 2009 to avoid a potential conflict of interest. She took a position with DHS's Office of Risk Management and Analysis on February 1, 2010.

Preface

The events of September 11, 2001, changed perceptions, rearranged national priorities, and produced significant new government entities, most notably the U.S. Department of Homeland Security (DHS). Whereas the principal mission of DHS is to lead national efforts to secure the nation against those forces that wish to do harm, the department also has responsibilities in regard to preparation for and response to other hazards and disasters, such as floods, earthquakes, and other "natural" disasters. Created in 2003, DHS is large and complex, with 22 "components," some of which were well established prior to the department's creation and others that were new creations along with the department. Across the department, whether in the context of preparedness, response, or recovery from terrorism, illegal entry to the country, or natural disasters, both the previous and the current DHS Secretaries have stated a commitment to processes and methods that feature risk assessment as a critical component for making better-informed decisions.

The difficulties in developing a risk-based framework and activities for decisions across DHS are daunting, largely due to the great uncertainties in understanding the suite of threats. In concept, however, risk assessment is believed to provide a good opportunity for sound analysis and consistent decision support. Against this backdrop, the U.S. Congress asked the National Research Council (NRC) of the National Academies to review and assess the activities of DHS related to risk analysis (P.L. 110-161, Consolidated Appropriations Act of 2008). Subsequently, a contract featuring the Statement of Task shown in Boxes S-1 and 1-1 was agreed upon by the National Academies and DHS officials to support this study. Our committee was appointed in October 2008 to carry out the study. The committee was a multidisciplinary group with technical, public policy, and social science expertise and experience concerning the areas of DHS's responsibilities.

During a 15-month study period, our full committee met 5 times and subgroups of the committee met another 11 times with DHS officials and representatives of a variety of organizations to gather information. (See Appendix C for a chronology of our meetings and visits and Appendix D for a list of individuals who contributed information and perspectives to our efforts.) At most of our meetings we received briefings from numerous DHS officials on various aspects of our charge.

The task of reviewing a large set of continually evolving activities across an organization as large and diverse as DHS presented difficulties for the committee. Although DHS is responsible for all aspects of homeland security, which

includes planning for and responding to natural disasters such as hurricanes, the report is weighted toward terrorism because that is where DHS efforts are weighted. Throughout, however, the committee was mindful of its chief objective: to help DHS by critiquing and providing advice on improving the risk-informed basis for decision making across the department. We began with a good appreciation for the difficulty of the task and that appreciation only grew as we learned more about relevant activities and their inherent challenges. We hope that this report is helpful to DHS as it proceeds with implementation of its plans.

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the NRC in making its published report as sound as possible and will ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report: John T. Christian, consulting engineer; Jared L. Cohon, Carnegie Mellon University; William H. Hooke, American Meteorological Society; Howard Kunreuther, Wharton Risk Management Center; Linda Landesman, New York City Health and Hospitals Corporation; Stephen M. Robinson, University of Wisconsin-Madison; Kathleen J. Tierney, University of Colorado at Boulder; Detlof von Winterfeldt, International Institute for Applied Systems Analysis; and Henry H. Willis, RAND Corporation.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Patrick Atkins, Pegasus Capital Investors (Retired) and Lynn R. Goldman, Johns Hopkins University. Appointed by the NRC, they were responsible for making certain that an independent examination of the report was carried out in accordance with institutional procedures and that all review comments were considered carefully. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Finally, I want to acknowledge and thank the committee members for their conscientious work, the help of DHS staff, and the dedicated work of the Academies staff.

John F. Ahearne, *Chair*

Contents

Acronyms

AEP	Annual Exceedance Probability
BARDA	Biomedical Advanced Research and Development Authority
BTRA	Biological Threat Risk Assessment
C2C	Cost-to-Capability
CAF	Critical Asset Factors
CBP	U.S. Customs and Border Protection
CBRN	Chemical, Biological, Radiological, Nuclear
CFATS	Chemical Facility Anti-Terrorism Standards
CIKR	Critical Infrastructure and Key Resources
CITA	Critical Infrastructure Threat Assessment Division (DHS)
CREATE	Center for Risk and Economic Analysis of Terrorism Events
CREM	Council for Regulatory Environmental Modeling (EPA)
CTRA	Chemical Terrorism Risk Assessment
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DOJ	Department of Justice
DoD	Department of Defense
EPA	Environmental Protection Agency
ERM	Enterprise Risk Management
EVPI	Expected Value of Perfect Information
EVPIX	Expected Value of Perfect Information About X
EVSI	Expected Value of Sample Information
GAO	Government Accountability Office
FEMA	Federal Emergency Management Agency
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HPS	Hurricane Protection System
HSGP	Homeland Security Grant Program
HSPD	Homeland Security Presidential Directive
I&A	Office of Intelligence & Analysis (DHS)
IP	Office of Infrastructure Protection (DHS)
iCBRN	Integrated Chemical, Biological, Radiological, Nuclear
ICE	Immigration and Customs Enforcement (DHS)
IECGP	Interoperable Emergency Communications Grant Program
IRMF	Integrated Risk Management Framework
IT	Information Technology
IVA	Infrastructure Vulnerability Assessment

MKB	Models Knowledge Base
MSRAM	Maritime Security Risk Analysis Model
NFIP	National Flood Insurance Program
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NMSRA	National Maritime Strategic Risk Assessment
NRC	National Research Council
OMB	Office of Management and Budget
PANYNJ	Port Authority of New York and New Jersey
PMI	Protective Measure Index
PPBE	Planning, Programming, Budgeting, and Execution
PRA	Probabilistic Risk Analysis
PSA	Protective Security Advisor
PSGP	Port Security Grant Program
QRA	Quantitative Risk Analysis
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RAPID	Risk Analysis Process for Informed Decision Making
RFI	Request for Information
RMA	Office of Risk Management and Analysis
RMAP	Risk Management Analysis Process
RMAT	Risk Management Analysis Tool
RMS	Risk Management Solutions
RRAP	Regional Resiliency Assessment Project
RSC	Risk Steering Committee (DHS)
S&T	Science and Technology Directorate (DHS)
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SHSP	State Homeland Security Program
SME	Subject Matter Expert
SSP	Site Security Plan
START	Study of Terrorism and Responses to Terrorism
SVA	Security Vulnerability Assessment
TCL	Target Capabilities List
TRAM	Terrorism Risk Assessment and Management
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program
TVC	Threat-Vulnerability-Consequences
UASI	Urban Areas Security Initiative
USCG	U.S. Coast Guard
USGS	U.S. Geological Survey
VOI	Value of Information
WMD	Weapons of Mass Destruction

Summary

In response to a request of the U.S. Congress (P.L. 110-161, Consolidated Appropriations Act of 2008), the National Research Council (NRC) established the Committee to Review the Department of Homeland Security's Approach to Risk Analysis to assess how the Department of Homeland Security (DHS) is building its capabilities in risk analysis to inform decision making. The specific tasks undertaken as the basis for the committee's assessment are listed in Box S-1. This summary presents the principal conclusions and the recommendations of the committee's full report.

SCOPE AND ROLE OF RISK ANALYSIS AT DHS

The scope of responsibilities of DHS is large, ranging over most, if not all, aspects of homeland security and supporting in principle all government and private entities that contribute to homeland security. For some functions, DHS is responsible for all of the elements of risk analysis. For other functions for which the responsibility is shared, effective coordination is required with owners and operators of private facilities; with state, territorial, and local departments of homeland security and emergency management; and with other federal agencies such as the Department of Health and Human Services, the Environmental Protection Agency, or the Department of Agriculture. While DHS is responsible for mitigating a range of threats to homeland security, including terrorism, natural disasters, and pandemics, its risk analysis efforts are weighted heavily toward terrorism, and that balance is reflected in this report.

Although risk analysis is just one input to decision making, it is an essential one. At DHS, risk analysis is used to inform decisions ranging from high-level policy choices to fine-scale protocols that guide the minute-by-minute actions of DHS employees. The committee focused its attention on risk analysis that informs the middle part of that spectrum, because it is for that range of decisions that technical improvements in risk analysis could have the greatest impact. Good risk analysis is also essential to creating decision rules for routine operations and for major policy choices, but in those cases non-technical considerations such as public acceptability can limit the potential value from improving capabilities for risk analysis. However, the recommendations offered in this report should also lead to improved inputs for those types of decisions.

BOX S-1
Statement of Task

The study will review how DHS is building its capabilities in risk analysis to inform decision making. More specifically, the study will address the following tasks:

a) Evaluate the quality of the current DHS approach to estimating risk and applying those estimates in its many management, planning, and resource-allocation (including grant-making) activities, through review of a committee-selected sample of models and methods;
b) Assess the capability of DHS risk analysis methods to appropriately represent and analyze risks from across the Department's spectrum of activities and responsibilities, including both terrorist threats and natural disasters;
c) Assess the capability of DHS risk analysis methods to support DHS decision-making;
d) Review the feasibility of creating integrated risk analyses covering the entire DHS program areas, including both terrorist threats and natural disasters, and make recommendations for best practices, including outreach and communications; and
e) Recommend how DHS can improve its risk analyses and how those analyses can be validated and provide improved decision support.

EVALUATION OF DHS RISK ANALYSIS CAPABILITIES

Approach to Study and Outline of Results

Based on its examination of six illustrative risk analysis models and processes—risk analysis of natural hazards, for critical infrastructure protection, and for allocation of homeland security grants; the Terrorism Risk Assessment and Management (TRAM) and Biological Threat Risk Assessment (BTRA) models; and DHS's Integrated Risk Management Framework—the committee came to the following primary conclusion:

Conclusion: DHS has established a conceptual framework for risk analysis (risk is a function of threat (*T*), vulnerability (*V*), and consequence (*C*), or *R = f(T,V,C)*) that, generally speaking, appears appropriate for decomposing risk and organizing information, and it has built models, data streams, and processes for executing risk analyses for some of its various missions. However, with the exception of risk analysis for natural disaster preparedness, the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested. Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability

that is sufficient to ensure reliable risk analyses other than for natural disasters.

Recommendation: To develop an understanding of the uncertainties in its terrorism-related risk analyses (knowledge that will drive future improvements), DHS should strengthen its scientific practices, such as documentation, validation, and peer review by technical experts external to DHS. This strengthening of its practices will also contribute greatly to the transparency of DHS's risk modeling and analysis. DHS should also bolster its internal capabilities in risk analysis as part of its upgrading of scientific practices.

A focus on characterizing sources of uncertainty is of obvious importance to improving the reliability of risk models and analysis as a basis for sound decision making. Uncertainties arise from missing or incomplete observations and data, imperfect understanding of the physical and behavioral processes that determine the response of natural and built environments and the people within them, subjectivity embedded within analyses of threat and vulnerability and in the judgments of what to measure among consequences, and the inability to synthesize data and knowledge into working models able to provide predictions where and when they are needed.

Proper recognition and characterization of both variability and uncertainty are important in all elements of a risk analysis, including effective interpretation of data as they are collected over time on threats, vulnerability, consequences, intelligence, and event occurrence. While some DHS work on risk does evaluate uncertainty, the uncertainties in their models and analyses were rarely mentioned by DHS risk analysts during the committee's meetings and site visits, and DHS appears to be at a very immature state with respect to characterizing uncertainty and considering its implications for ongoing data collection and the prioritization of efforts to improve methods and models. Closely tied with the topic of characterizing uncertainty is that of representing properly the precision of risk analyses.

The conclusion above about the capability of DHS risk analysis methods to support decision making is based on the committee's assessment of the quality of those methods, in response to element (c) of the statement of task. Quality was evaluated in two ways, in accordance with elements (a) and (b) of the task, which overlap. The committee interpreted the first element ("Evaluate the quality of the current DHS approach to estimating risk and applying those estimates. . .") as calling for an assessment of general frameworks and the second ("Assess the capability of DHS risk analysis methods to appropriately represent and analyze risks . . .") as requiring an assessment of actual implementations. The committee concluded that the basic framework of risk analysis used by DHS is sound but that the operationalization of that framework is in many cases seriously deficient, as indicated in more detail below in this Summary and as supported by Chapters 4 and 5 of the report.

The committee reviewed the feasibility of creating integrated risk analyses

covering the entire DHS program areas (element (d) of the task) and concluded that it is not advisable. Instead, the committee recommends in the section "Integrated Risk Analyses," below, that DHS perform comparative risk analyses. The distinction is explained in that section of this Summary and in Chapter 4 of the report. The final element of the task calls for the committee to recommend steps for improvement, and these are captured in recommendations throughout this Summary and in the main text of the report.

Natural Hazards Risk Analyses

There is a solid foundation of data, models, and scholarship to underpin DHS's risk analyses for natural hazards such as flooding. Although models are constantly being developed and improved, risk analysis associated with natural hazards is a mature activity—compared to risk analysis related to terrorism—in which analytical techniques are subject to adequate quality assurance and quality control, and verification and validation procedures are commonly used.

Conclusion: DHS's risk analysis models for natural hazards are near the state of the art. These models—which are applied mostly to earthquake, flood, and hurricane hazards—are based on extensive data, have been validated empirically, and appear well suited to near-term decision needs.

Recommendation: DHS's current natural hazard risk analysis models, while adequate for near-term decisions, should evolve to support longer-term risk management and policy decisions. Improvements should be made to take into account the consequences of social disruption caused by natural hazards; address long-term systemic uncertainties, such as those arising from effects of climate change; incorporate diverse perceptions of risk impacts; support decision making at local and regional levels; and address the effects of cascading impacts across infrastructure sectors.

Infrastructure Risk Analyses

The risk analyses that DHS conducts in support of infrastructure protection generally decompose risk into threat (T), vulnerability (V), and consequences (C). With respect to risk from terrorism, defining the threat and estimating probabilities are inherently challenging because of the lack of experience with such events; the associated absence of data on which to base reliable estimates of probabilities; and the effects of an intelligent adversary that may seek to defeat preparedness and coping measures, which causes T, V, and C to be interdependent. There are various methods to compensate for the lack of historical data, including "red team" analyses (in which experts are charged with trying to overcome risk-mitigation measures), scenario analysis, and subject-matter ex-

pert (SME) estimates, and DHS has pursued most of these, although not as consistently as would be desired. There are also multiple methods for combining estimates of threats, vulnerabilities, and consequences and dealing with the dependencies of *T*, *V*, and *C* to estimate risk, such as Bayesian analysis, multi-attribute models, attacker-defender models, or game theoretic calculations. DHS has generally not applied these methods.

DHS's analyses of vulnerabilities has focused primarily on physical vulnerabilities. There are significant areas to expand this approach to more consistently cover the span of threats. For example, DHS's vulnerability analyses rarely address coping capacity and resilience (or long-term adaptation). People-related factors, a major part of coping capacity, have been largely overlooked.

Similarly, DHS analyses of consequences have tended to focus on the outcomes that are most readily quantified. Little attention has been paid to secondary economic effects or to an attack's effects on personal and group behaviors—impacts that could be significant and may be the primary goals of terrorists. Some relevant research is being conducted in DHS's University Centers of Excellence, and a small amount is funded by the Human Factors and Behavioral Sciences program within DHS's Science and Technology Directorate, but much more is needed. In addition, efforts must be made to incorporate the results of such research into DHS risk analyses and to heighten risk analysts' awareness of the importance of social and economic impacts.

Recommendation: DHS should have a well-funded research program to address social and economic impacts of natural disasters and terrorist attacks and should take steps to ensure that results from the research program are incorporated into DHS's risk analyses.

Based on its study, the committee concluded that DHS's risk analyses for infrastructure protection might be useful but certainly can be improved. Improvements can be made by considering the adaptability of intelligent adversaries, consistently including evaluation of non-physical vulnerabilities, characterizing sources of uncertainty, working toward verification and validation of models, improving documentation, and by submitting models and analyses to external peer review.

Recommendation: DHS should consider alternatives to modeling the decisions of intelligent adversaries with fixed probabilities. Models that incorporate game theory, attacker-defender scenarios, or Bayesian methods to predict threat probabilities that evolve over time in response to observed conditions and monitored behavior provide more appropriate ways of representing the decisions of intelligent adversaries and should be explored.

Recommendation: DHS should ensure that vulnerability and consequence analyses for infrastructure protection are documented, transparent, and repeatable. DHS needs to agree on the data inputs, understand the technical approaches used in models, and understand how the models are calibrated, tested, validated, and supported over the life cycle of use.

Homeland Security Grants

The committee's evaluation of the risk-based homeland security grant programs administered by the Federal Emergency Management Agency (FEMA) within DHS determined that they are reasonably executed, given political and other practical considerations. Population counts serve, for the most part, as the surrogate measure for risk. Some of the grants programs are moving toward risk-based decision support, but the various approaches and formulas are still evolving.

Recommendation: FEMA should undertake an external peer review by technical experts outside DHS of its risk-informed formulas for grant allocation to identify any logical flaws with the formulas, evaluate the ramifications of the choices of weightings and parameters in the consequence formulas, and improve the transparency of these crude models of risk.

Recommendation: FEMA should be explicit about using population density as the primary determinant for grant allocations.

Terrorism Risk Assessment and Management Model

DHS's Terrorism Risk Assessment and Management (TRAM) model is held up as a successful instantiation of risk analysis, and the Port Authority of New York and New Jersey (which initiated TRAM's development even before the establishment of DHS) is a satisfied user. The committee has concerns, however, owing to the model's unjustified complexity and lack of validation.

Recommendation: DHS should seek expert, external peer review of the TRAM model in order to evaluate its reliability and recommend steps for strengthening it.

Biological Threat Risk Assessment Model

DHS's Biological Threat Risk Assessment (BTRA) model, which is used to create biennial assessments of the risks of biological terrorism, was thoroughly reviewed in an NRC report published in 2008.[1] The primary recommendation of that report reads as follows:

> The BTRA should not be used as a basis for decision making until the deficiencies noted in this report have been addressed and corrected. DHS should engage an independent, senior technical advisory panel to oversee this task. In its current form, the BTRA should not be

[1] National Research Council (2008).

used to assess the risk of biological, chemical, or radioactive threats. (p. 5)

The committee was told by DHS that it is addressing most of the recommendations of the 2008 NRC review, but in the committee's view the response has been incremental, and a much deeper change is necessary. DHS's proposed responses will do little to reduce the BTRA model's great complexity, which requires many more SME estimates than can be supported by the limited base of knowledge about biological terrorism. It also precludes transparency, adequate sensitivity analysis, and validation.

Integrated Risk Management Framework

The establishment of the Integrated Risk Management Framework (IRMF) across DHS is going in the right direction, but it is far too early to know if the IRMF will provide real value. Similar integrated or enterprise-level risk management processes in industry typically require several years before their benefits begin to appear. The committee did not observe any improvements to DHS's risk analysis that could be attributed to these early steps, and so it concludes that integrated risk management may be on the right track but is early in development.

Crosscutting Modeling Issues

Transparency

Transparency is always important in risk analysis, and especially so when analysts and decision makers must contend with great uncertainty, as is the case with the risks posed by terrorism. The committee found that most DHS risk models and analyses are quite complex and poorly documented, and thus are not transparent to decision makers or other risk analysts. Moreover, some of those models imply false precision, which can give the impression of certainty when it does not exist. Security restrictions are another contributor to poor transparency in some cases.

Recommendation: To maximize the transparency of DHS risk analyses for decision-makers, DHS should aim to document its risk analyses as clearly as possible and distribute them with as few constraints as possible. Further, DHS should work toward greater sharing of vulnerability and consequence assessments across infrastructure sectors so that related risk analyses are built on common assessments.

Risk Communication

DHS's IRMF and National Strategy for Information Sharing documents focus on sharing information with decision makers. However, it is essential that communication with stakeholders and the general public also be included in a comprehensive risk communication strategy. For risks to be truly managed, DHS needs to provide not only information but also analysis and aids to thinking that prepare all affected audiences to cope better with the risks that events might entail. As DHS moves to the next stages of risk communication—which will have to go far beyond information sharing and include a capability for understanding the perceptions and needs of the recipients of various risk-related communications and for translating that understanding to specifically tailored messages—a well-developed risk communication strategy document and program, adequately staffed and funded, will be needed.

Integrated Risk Analyses

DHS is working toward risk analyses that are increasingly comprehensive, in an attempt to enable comparison of the diverse risks under the department's purview. The committee evaluated the feasibility of creating integrated risk analyses that span all of DHS's areas of responsibility. An integrated risk analysis collects analyses for all potential risks that an entity, here DHS, is charged with assessing and combines those risks into one complete analysis based on a common metric. A comparative risk analysis, by contrast, omits that last step. In comparative risk analysis, potential risks to an entity from many different sources are analyzed and the risks then compared (or contrasted), but no attempt is made to assess them against a common metric.

Qualitative risk analysis includes methods for formally eliciting advice (such as Delphi analysis and expert judgment) for use in decision making. Such advice can be used to *compare* risks of very different types. There is a well-established literature on comparative risk analysis that can be used to apply the TVC approach to different types of risk.[2] Importantly, the results of such analysis are likely to involve substantially different metrics that cannot be directly compared. In addition, the degree and the extent of uncertainty are likely to be very different across the various risk sources. Nonetheless, the scope and diversity in the metrics can be very informative for decision making as well.

Conclusion: A fully integrated analysis that aggregates widely disparate risks by use of a common metric is not a practical goal and in fact is

[2] For example, see Fischhoff (1995), Florig et al. (2001), Morgan et al. (1996), Willis et al. (2004), Davies (1996), Finkel and Golding (1994), and U.S. Environmental Protection Agency (1987).

likely to be inaccurate or misleading given the current state of knowledge of methods used in quantitative risk analysis. The risks presented by terrorist attack and natural disasters cannot be combined in one meaningful indicator of risk, and so an all-hazards risk assessment is not practical. The science of risk analysis does not yet support the kind of reductions in diverse metrics that such a purely quantitative analysis would require. Qualitative comparisons can help illuminate the discussion of risks and thus aid decision makers.

Recommendation: DHS should not attempt an integrated risk assessment across its entire portfolio of activities at this time because of the heterogeneity and complexity of the risks within its mission.

The committee is more optimistic about using an integrated approach if the subject of the analysis is a set of alternative options for managing risk—for example, if the analysis is of alternative investments for improving resilience. In such cases, the same option might prove able to reduce risks arising from a number of sources such as natural hazards and terrorism. The analysis of alternative risk management options for mitigating risks to a set of activities or assets could then be accomplished through a single quantitative model in much the same way that cost-effectiveness analysis can be used to select a least-cost investment even when the benefits of the various options are incommensurate.

THE PATH FORWARD—RECOMMENDED ACTIONS

Improve the Way Models Are Developed and Used

The committee observed a tendency across most of DHS to build and use complex quantitative models in the apparent belief that such models are the best way to approach risk analysis. Effective risk analysis need not always be quantitative. In particular, the generation and analysis of scenarios is an important component of risk assessment and management in a number of fields. In some cases, improved understanding of risks hinges on improved communication, organizational design, and so on.

The multiple dimensions of risk associated with natural hazards and terrorism are now widely recognized in the risk literature. These include public health and safety, as well as social, psychological, economic, political, and strategic aspects. The desire to quantify, compare, and rank risks arising from different sources can lead to characterizations that simplify or ignore many of these dimensions. In several of the risk studies presented to it, the committee observed omissions and oversimplifications of this type, reflecting a tendency to ignore non-quantifiable risks and to combine non-commensurate attributes into single measures of consequence. Even though DHS is not responsible for managing all aspects of risk—for example, the Department of Health and Human Services has the primary responsibility for managing public health risks—it is appropriate

and necessary to consider the full spectrum of consequences when performing risk analyses intended to inform constructive and effective decision making.

Recommendation: In characterizing risk, DHS should consider a full range of public health, safety, social, psychological, economic, political, and strategic outcomes. When certain outcomes are deemed unimportant in a specific application, reasons for omitting this aspect of the risk assessment should be presented explicitly. If certain analyses involve combining multiple dimensions of risk (e.g., as a weighted sum), estimates of the underlying individual attributes should be maintained and reported.

The committee observed that DHS relies heavily on quantitative models for its risk analysis activities. This approach reflects an outdated and oversimplified view of risk analysis and is certain to result in underemphasizing many attributes of risk that cannot be readily quantified, such as differences in individual values. Instead, risk analysis should be regarded as having both quantitative and non-quantitative attributes, and it should be recognized that narrative descriptions of non-quantitative information about risk are often as important to decision makers as is the more fully quantitative information. Although there are certainly decisions that can be fully informed by the use of simple, quantitative models, it is the case that many important decisions require understanding of the multiple attributes integral to risk. This last point emphasizes that careful delineation of the different types of decisions that DHS has to make is an important precursor to understanding the types of risk analyses appropriate for informing those decisions.

Recommendation: DHS should prepare scientific guidelines for risk analyses recognizing that different categories of decisions require different approaches to risk analysis strict reliance on quantitative models is not always the best approach.

To start, DHS should examine the basic structure of its risk analysis approach. Currently, DHS seems to use the special case formula Risk = $T \times V \times C$ very broadly for both terrorism and natural hazards applications. DHS needs to be very careful in documenting assumptions and understanding when the multiplicative formula is appropriate and when it is not.

Risk as a function of *interdependent variables* T, V, and C is a reasonable problem decomposition for analysis of risks posed by both terrorism and natural hazards. In the natural hazards domain, independence can sometimes be assumed to hold among components, and the formula can be reduced to Risk = $T \times V \times C$. In the more general case for natural hazards, the three components may not be independent but the nature of their interdependence may be reasonably known and subject to analysis. In the terrorism domain, however, it is often the case that T, V, and C are functionally interdependent, so that the simple risk function $R = T \times V \times$ C does not apply and should not be used. In particular,

DHS must examine clearly whether the variables *T*, *V*, and *C* are actually independent and must guard against the errors that can occur when independence is wrongly assumed.

Conclusions:

1. The basic risk framework of Risk = *f*(*T*,*V*,*C*) used by DHS is sound and in accord with accepted practice in the risk analysis field.

2. DHS's operationalization of that framework—its assessment of individual components of risk and their integration into a measure of risk—is in many cases seriously deficient and is in need of major revision.

3. More attention is urgently needed at DHS to assessing and communicating the assumptions underlying and the uncertainties surrounding analyses of risk, particularly those associated with terrorism.

Until these deficiencies are improved, only low confidence should be placed in most of the risk analyses conducted by DHS.

Follow Time-Tested Scientific Practices

DHS has not been following the critical scientific practices of documentation, validation, peer review by technical experts external to DHS, and publishing. Given the lack of that disciplined approach, it is very difficult to know precisely how DHS risk analyses are being done and whether their results are reliable and useful in guiding decisions. There is little understanding of the uncertainties in DHS risk models other than those for natural hazards, and in addition there is a tendency toward false precision. It is one thing to evaluate whether a risk model has a logical purpose and structure—the kind of information that can be conveyed through a briefing—but quite another to really understand the critical inputs and sensitivities that determine whether or not it truly produces reliable outputs. The latter understanding comes from scrutiny of the mathematical model, evaluation of a detailed discussion of the model's implementation, and review of some model results, preferably when compared against simple bounding situations and potentially retrospective validation. It is not adequate to simply ask subject-matter experts whether they see anything odd about a model's outcomes.

The committee found that in general the models and methods it reviewed did not have the capability to appropriately represent and analyze risks from across the department's spectrum of activities and responsibilities. As part of its review, the committee addressed what was lacking in the models and methods. It often found that little direct, and more importantly, little effective attention was paid to the features of the risk problem that are fundamental to the homeland security modeling purview. For example, throughout its review, the committee was concerned about the lack of state-of-the-art risk modeling in address-

ing key homeland security issues such as vulnerability, intelligent adversaries, and the range of socioeconomic consequences.

As a result, the committee questions whether the creation of the department from many existing organizations with long-standing approaches to risk analysis might have anchored the DHS to the legacy models of its components. In such cases, and with no de novo process to develop methods and models that specifically focus on the new factors characterizing homeland security risks, it would not be surprising to find a poor fit between legacy models and the demands of a substantially new application. Moreover, if legacy modeling is in fact the source of the capability deficiency, then the committee found little evidence in the materials reviewed that DHS has considered, much less rigorously addressed, this general issue of model design.

Recommendation: DHS should adopt recognized scientific practices for its risk analyses:

- **DHS should create detailed documentation for all of its risk models, including rigorous mathematical formulations, and subject them to technical and scholarly peer review by experts external to DHS. Documentation should include simple worked-out numerical examples to show how a methodology is applied and how calculations are performed.**
- **DHS should consider creating a central repository to enable DHS staff and collaborators to access model documentation and data.**
- **DHS should ensure that models undergo verification and validation—or sensitivity analysis at the least. Models that do not meet traditional standards of scientific validation through peer review by experts external to DHS should not be used or accepted by DHS.**
- **DHS should use models whose results are reproducible and easily updated or refreshed.**
- **DHS should continue to work toward a clear, unambiguous risk lexicon.**

Discard the Idea of a National Risk Officer

The director of DHS's Office of Risk Management and Analysis (RMA) suggested to the committee that the DHS Secretary, who already serves as the Domestic Incident Manager during certain events, could serve as the "country's chief risk officer," establishing policy and coordinating and managing national homeland security risk efforts.[3] A congressional staff member supported the

[3] Presentation by Tina Gabbrielli, RMA director, at the second committee meeting, February 4-5, 2009, Washington, D.C.

concept of establishing a chief risk officer.[4] The committee has serious reservations about this idea. Risk is assessed for many issues across many federal agencies, to address disparate concerns such as health effects, technology impacts, and the safety of engineered systems. The approaches taken differ depending on the issues and the agency missions, and they require disciplinary knowledge ranging from detailed engineering and physical sciences to social sciences and law. For a single entity to wisely and adequately bring to bear such a broad range of expertise to address wide-ranging issues would require a large, perhaps separate agency. In addition, as other NRC studies have concluded, risk analysis is done best as a result of interactions between the risk analysts and the stakeholders, including the involved government agencies. To be effective, such interactions require that the federal agents have an understanding of the issues and of the values of the stakeholders. An attempt to locate all this expertise and experience in one department and to require that the personnel stay current in many different areas is unlikely to succeed.

Build a Strong Risk Analysis Culture at DHS

The long-term effectiveness of risk analysis throughout DHS and the improvement of scientific practice to enable such success both depend on the continued development of an adequate in-house workforce of well-trained risk analysis experts. As DHS expands its commitment to risk analysis, personnel who are up-to-date on scientifically grounded methods for carrying out such analyses will be in increasing demand. At present, DHS is heavily dependent on private contractors, academic institutions, and government laboratories for the development, testing, and use of models; acquisition of data for incorporation into models; interpretation of results of modeling efforts; and preparation of risk analyses. Although there are advantages to relying on expertise that is not available within DHS, in-house specialists should be fully aware of the technical content of such work. In particular, in-house DHS personnel need to ensure the scientific integrity of the approaches and understand the uncertainties inherent in the data, the risk models, and the products of those models. Contractor support will remain essential, but the direction and application of such work should be under the tight control of in-house staff.

Recommendation: DHS should have a sufficient number and range of in-house experts, who also have adequate time, to define and guide the efforts of external contractors and other supporting organizations. DHS's internal technical expertise should encompass all aspects of risk analysis, including the social sciences. DHS should also evaluate its dependence on contractors and the possible drawbacks of any proprietary arrangements.

[4] Presentation by Michael Beland, House of Representatives Homeland Security Committee staff member, at the second committee meeting, February 4-5, 2009, Washington, D.C.

Recommendation: DHS should convene an internal working group of risk analysis experts to work with its Risk Management and Analysis and Human Resource offices to develop a long-term plan for the development of a multidisciplinary risk analysis staff throughout the department and practical steps for ensuring such a capability on a continuing basis. The nature and size of the staff, and the rate of staffing, should be matched to the department's long-term objectives for risk-based decision making.

1
Introduction

The U.S. Congress asked the National Research Council (NRC) of the National Academies to review and assess the activities of the Department of Homeland Security (DHS) related to risk analysis (P.L. 110-161, Consolidated Appropriations Act of 2008). Subsequently, a contract featuring Statement of Task in Box 1-1 was agreed upon by the National Academies and DHS officials to support this study. A committee was appointed in October 2008 to carry out the study.

Elements (a)-(c) of this task are intertwined, because the capability of risk analysis methods to "represent and analyze risks" and to "support … decision-making" are inherent in any evaluation of the quality of risk analysis. Therefore, the committee addressed these three task elements as multiple lenses through which to examine the "committee-selected sample of models and methods," and it interpreted task (a) as the overarching goal of the study, with tasks

BOX 1-1
Statement of Task

The study will review how DHS is building its capabilities in risk analysis to inform decision-making. More specifically, the study will address the following tasks:

a) Evaluate the quality of the current DHS approach to estimating risk and applying those estimates in its many management, planning, and resource-allocation (including grant-making) activities, through review of a committee-selected sample of models and methods;

b) Assess the capability of DHS risk analysis methods to appropriately represent and analyze risks from across the Department's spectrum of activities and responsibilities, including both terrorist threats and natural disasters;

c) Assess the capability of DHS risk analysis methods to support DHS decision-making;

d) Review the feasibility of creating integrated risk analyses covering the entire DHS program areas, including both terrorist threats and natural disasters, and make recommendations for best practices, including outreach and communications; and

e) Recommend how DHS can improve its risk analyses and how those analyses can be validated and provide improved decision support.

(b) and (c) as particular points of emphasis. All three of these task elements were addressed through careful examination of an illustrative set of models and methods (see below), because it would be impossible to review the scores of DHS risk models and processes in a timely fashion. Through this sampling approach, the committee was exposed to major risk analysis activities across DHS and saw many commonalities. Although DHS is responsible for a range of threats to homeland security, including terrorism, natural disasters, and pandemics, its risk analysis efforts are heavily weighted toward terrorism, and that balance is reflected in this report.

Since its formation in 2002, DHS has espoused the principle of risk-informed decision making. The current DHS Secretary underscored the importance of risk analysis as follows:

> Development and implementation of a process and methodology to assess national risk is a fundamental and critical element of an overall risk management process, with the ultimate goal of improving the ability of decision makers to make rational judgments about tradeoffs between courses of action to manage homeland security risk.[1]

For the purposes of this study, the committee accepted the definition of "risk analysis" found in the glossary of the Society for Risk Analysis:

> A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.[2]

In contrast to some definitions, this version does not explicitly include risk perception and risk communication, though the latter are clearly important elements if risk analysis is to be effective.

THE DECISION-MAKING CONTEXT FOR THIS STUDY

The Statement of Task emphasizes the role of risk analysis as support for decision making. Risk analysis is not done in a vacuum; it is framed according to the decisions it will inform, and the results are made available in the form needed by the decision makers.

At DHS, risk analysis is used to inform decisions ranging from high-level policy choices to fine-scale protocols that guide the minute-by-minute actions of DHS employees. To illustrate these different levels of decision making, a policy

[1] Janet A. Napolitano, Terms of Reference, 2009 Quadrennial Homeland Security Review.
[2] See *http://www.sra.org/resources_glossary_p-r.php*. Accessed January 22, 2010.

decision related to our borders might call for strengthening the borders. With that policy in place, decisions might include setting the level of resources to be allocated to U.S. Customs and Border Protection (CBP) and deciding which border segments require extra attention. Finer-scale decisions might choose from among different options for upgrading enforcement along those segments—choosing, for example, from among different combinations of staffing, surveillance, biometrics, and so on. Finally, decision rules must be created for triggering extra checks and deciding when to pursue enforcement actions.

The committee focused its attention on risk analysis that informs the middle part of that spectrum, whether the decision making is done within DHS or at a DHS partner entity that actually "owns" and manages a given risk. This focus is in large part because the risk analyses that contribute to decision rules for routine operations and for major policy choices are especially tempered by non-technical aspects such as public perception and privacy, which, while not at all undermining the importance of solid risk analyses, do complicate an external review of the process that led to those rules. By contrast, the range of decisions on which the study focused could see the greatest improvement if risk analysis is strengthened. Improving the quality of risk analysis in general will also lead to better inputs for policy and decision rules for routine operations.

Non-routine decisions, such as how to respond to a particular threat situation or how to prepare security for a major national event, usually are unique in character, requiring special approaches that cannot be anticipated. These preparations are driven more by the experience of security experts than by any risk analysis that the committee would be able to examine a priori. Nevertheless, some of the principles set forth in this report should be of value to those decisions as well.

Risk analysis is just one input to decision making, although it is an essential one. Yet ultimately decisions are made by risk managers, who must overlay the analyses with considerations of a pragmatic, political, or other character. Risk analysis does not make decisions, it informs them: the analysts cannot build a calculus that balances all relevant considerations. However, this is not to say that risk analysis and risk management (decision making) are, or should be, in separate compartments or stovepipes. Instead, those functions should engage in back-and-forth interplay. Analysts need to have a clear understanding of the decisions to be made and the considerations beyond analysis that will be folded in. Decision makers must have a good understanding of the capabilities and limitations of risk analysis: indeed, it is the responsibility of risk analysts to ensure that they do. The emphasis of the Statement of Task on informing and supporting decision making, and its mention of "outreach and communications" reflect that interplay. Whether management of a given risk is vested within DHS or handled elsewhere, it is essential that DHS risk analysis reach out to effect good risk management.

RISK MODELS AND METHODS EXAMINED IN DETAIL TO CARRY OUT THIS STUDY

Chapter 2 gives an overview of risk analysis at DHS, which is effected with the help of—by DHS's count—some 60 risk models and processes. At its first two meetings, the committee was briefed on approximately a dozen of those models and processes. Based on those briefings and the experience of its members, several site visits were planned, at which subsets of the committee learned about some of the models and processes—and additional ones—in more detail. DHS acknowledged that some of the models and processes in its count were at an early stage of development and therefore not good illustrations of DHS's capability in risk analysis. As stipulated in the Statement of Task, the committee selected an illustrative sample of risk models and methods to examine in detail in order to carry out the study's evaluation. Its criteria were that the models and processes selected be at least somewhat mature; documented to some extent and; used for a major DHS purpose rather than a niche application and that the set collectively spans the major DHS functions of infrastructure protection, support to first responders, transportation risks, and understanding the risks of weapons of mass destruction and of natural disasters. Guided by those criteria, the committee selected the following sample set:

- Risk analysis done by DHS with respect to natural hazards, as exemplified by the flood frequency estimates and floodplain maps that the Federal Emergency Management Agency (FEMA) produces to inform the National Flood Insurance Program.[3] This is a mature process grounded in extensive historical data and commonly accepted statistical models.
- Threat, vulnerability, and consequence analyses performed for the protection of critical infrastructure and key resources (CIKR). This work is done in or for the DHS Office of Infrastructure Protection (IP), which carries out these analyses to inform decision making with respect to the nation's CIKR assets. This is one of the major responsibilities assigned to DHS when it was established. The management of risks for CIKR is the responsibility of particular DHS components, other federal agencies, and many private owners and operators. Perhaps for that reason, IP does not generally integrate the pieces to develop risk analyses, but instead produces these component analyses. Much of the vulnerability analysis within IP is handled by Argonne National Laboratory, and much of the consequence analysis is handled by the National Infrastructure Simulation and Analysis Center (NISAC), a joint program of Sandia National Laboratories and Los Alamos National Laboratory.
- Risk models used to underpin those DHS grant programs for which al-

[3] DHS, through FEMA, is responsible for assessments of flood risk, but DHS does not conduct risk analyses for most other natural disasters. As an illustration of how DHS performs risk analysis for natural hazards, this report focuses on flood risk because the analyses in that case are within DHS's purview.

locations are based on risk. These programs are administered by FEMA within constraints set by Congress, and they have a broad and widespread effect on the nation's preparedness. Key elements of the modeling are done by a contractor.

- The Terrorism Risk Assessment and Management (TRAM) tool. This is a mature software-based method for performing risk analysis primarily in the transportation sector. It has been in use at the Port Authority of New York and New Jersey for about a decade, so there is a good deal of experience to inform the committee's evaluation of its quality and capabilities. The development of TRAM was initiated by the Port Authority, with initial funding from the Department of Justice, and the work has been done by a contractor. TRAM appears to share the general structure of other risk analysis tools such as the Maritime Security Risk Analysis Model (MSRAM) and the Risk Analysis and Management for Critical Asset Protection (RAMCAP) and RAMCAP Plus, although the committee did not examine the particular details of those tools.
- The Biological Threat Risk Assessment (BTRA) is a large-scale, complex, event-tree formulation created by a contractor with DHS funding. It is meant to inform decision making by the White House Homeland Security Council, the Department of Health and Human Services, and others. The general BTRA approach appears to be similar to the approach used for DHS's Chemical Terrorism Risk Assessment (CTRA) model and its Integrated Chemical, Biological, Radiological, Nuclear (iCBRN) assessment, though the committee did not examine the details of these models to determine the degree of similarity. BTRA was the subject of a thorough NRC review (2008), captured in *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*, from which the committee drew heavily.
- The Integrated Risk Management Framework (IRMF). The IRMF is not a particular risk model, but it fits within the category of "methods" in element (a) of the Statement of Task. The committee examined IRMF as it is being developed by DHS's Office of Risk Management and Analysis (RMA), which is working to coordinate risk analysis across the department. RMA's development of IRMF and supporting elements generally follows implementation of Enterprise Risk Management (ERM) in the private sector, aligning most closely with ERM practices found in nonfinancial services companies. The committee was told by RMA that the U.S. Coast Guard and Immigrations and Customs Enforcement also practice, or are developing, similar ERM approaches within their component agencies, but did not examine those efforts.

Collectively, this sample captures models and processes spanning a range of maturity—some predating the establishment of DHS, up to the IRMF, which is still under development. The sample includes programs such as those for infrastructure protection and grant allocation that are major activities of DHS informing billions of dollars of outlays. This sample of models and methods exposed the committee to the work of a broad range of DHS risk experts, including major contractors who contribute to DHS's risk analyses. Through the BTRA, the committee examined a major, high-profile effort to assess the risks of weapons

of mass destruction, and through TRAM, the committee saw how DHS works with an experienced quasi-governmental entity. This sample captures methods that are influential in DHS and which collectively inform a very broad set of homeland security decision making. During the course of the study, the committee was also exposed to other risk analysis efforts within DHS, such as an agent-based simulation tool being developed by the Transportation Security Administration and one of its contractors and the Coast Guard's Maritime Security Risk Analysis Model. The committee did not attempt to draw inferences from those limited exposures.

HOW THE STUDY WAS CONDUCTED

To carry out its charge, the full committee met five times and subgroups of the committee went on 11 site visits (see Appendixes C and D). The breadth of DHS precluded an exhaustive examination of risk analysis across the department, so the committee relied on RMA to identify topics and speakers for its first two meetings. Those meetings provided an introductory survey. The committee examined RMA's inventory of some 60 risk models and practices across DHS, familiarized itself with studies from the Government Accountability Office (GAO) and the Congressional Research Service and with DHS publications, and used the committee members' knowledge of DHS and suggestions from congressional staff to decide on other topics to explore or programs to examine in more detail. The committee decided to focus on risk analysis that was mature enough for some degree of sophistication to be expected. It put its emphasis on risk analysis programs with high visibility or that contribute to major parts of DHS's counterterrorism and natural disasters missions. Because DHS risk analysis practices have evolved from different roots—some building on practices in the security community, some emulating business risk management practices, and some adapting concepts and tools from engineering—the committee explored the range of risk cultures within DHS. It also made special efforts to discern how well DHS risk analyses and tools support risk management outside DHS.

The site visits enabled subsets of the committee to engage in in-depth interactions with staff members from several DHS offices and programs and also to collect insights from some of DHS's risk management partners. Site visits were made to the following operations:

- Port Authority of New York and New Jersey
- Environmental Protection Agency (EPA) headquarters office in charge of the agency's homeland security activities
- EPA National Homeland Security Research Center
- Department of Health and Human Services offices that deal with preparedness

- DHS's IP and Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) programs
- NISAC
- North Carolina Department of Homeland Security
- FEMA's Grant Program Directorate
- Naval Postgraduate School Department of Operations Research
- A Fusion Center Conference

STRUCTURE OF THIS REPORT

Chapter 2 describes DHS's current systems for risk analysis. Chapter 3 discusses some of the general challenges facing DHS risk analysis, and Chapter 4 provides the committee's evaluation of those capabilities and makes recommendations for improvements. Chapter 5 provides more general recommendations for moving forward to create a strong culture of risk analysis throughout DHS.

Elements (a)-(c) of the Statement of Task are covered in Chapter 4, which presents evaluations of illustrative DHS risk analysis models and evaluations of cross-cutting issues that affect their quality; the dimensions of quality referred to in task elements (b)-(c) are reflected in the overall assessments of quality. Element (b) is addressed in a more targeted fashion in the sections of Chapter 5 that deal with the basic structure of DHS risk models, the need for strong scientific practice, and the need for improving the technical capabilities of DHS staff with respect to risk analysis. Element (c) is addressed in a more targeted way in the subsection of Chapter 4 titled "The Assumptions Embedded in Risk Analyses Must Be Visible to Decision Makers." However, the emphasis on risk analysis serving the needs of decision-makers is discernible throughout this report. The several questions raised in element (d) of the Statement of Task are addressed in Chapter 4's subsections on "Comparing Risks Across DHS Missions" and "Toward Better Risk Communication," in Chapter 4. Task (e) is addressed by the entirety of Chapter 5. In particular, the necessary (though not sufficient) step for DHS risk analyses to be validated and provide better decision support is for work to begin on characterization of the uncertainties in all the models and processes. The committee's overall evaluation of the quality of DHS risk analysis capabilities is provided in the last conclusion in Chapter 4.

2
Overview of Risk Analysis at DHS

INTRODUCTION

The scope of responsibilities of the Department of Homeland Security (DHS) is substantial. Responsibilities range over most, if not all, aspects of homeland security and support in principle all government and private entities that contribute to homeland security. DHS is directly responsible for the planning for and recovery from nearly any catastrophic disaster, whether human inflicted or naturally occurring. The mission encompasses the following elements:

- Terrorism and natural hazards (e.g., see p. 3 of *http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf*; natural hazards were emphasized also by Homeland Security Presidential Directive 5 [HSPD-5] *http://www.dhsgov/xabout/laws/gc_1214592333605.shtm*);
- Border patrol and immigration;
- Criminal activities within the jurisdiction of crimes that Immigration and Customs Enforcement (ICE), the U.S. Secret Service, and the U.S. Coast Guard (USCG) are responsible for;
- Marine safety and protection of natural resources within the responsibility of the USCG;
- Cyber security (HSPD-7, available online at *http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm*); and
- Accidental hazards, a term that encompasses industrial and commercial accidents with the potential to cause widespread damage to or disruption of economic and social systems.

DHS includes 22 major "components," many of which are well-known and long-standing federal organizations. The DHS organization chart (with some identified risk models and tools by directorate) is shown in Figure 2-1; the risk acronyms are spelled out in Table 2-1. It is clear then that DHS has a complicated responsibility with multiple functions, often only loosely related. This is reflected in DHS's very broad definition of risk (DHS-RSC, 2008):

> The Department of Homeland Security (DHS) defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. These risks arise from potential acts of terrorism, natural dis-

> asters, and other emergencies and threats to our people and economy, as well as violations of our borders that threaten the lawful flow of trade, travel, and immigration.

It is also clear that risk analysis is an activity that is spread broadly across DHS. This complexity and breadth distinguish DHS from many organizations that have successfully adopted risk analysis to inform decision making.

THE DECISION CONTEXT AT DHS

Regarding the types of decisions that effective risk management analysis might support, Figure 2-2 illustrates risk-informed decisions that confront DHS as defined by their time horizons. Decisions on the far left side of the figure are pure policy level decisions, such as how to balance the overall DHS focus among terrorism, law enforcement, infrastructure protection, preparedness-emergency response, and so forth. These address judgments that rely heavily on factors beyond just science and engineering.

The type and volume of data available tend to change from qualitative and subjective to quantitative and objective as one moves from left to right in Figure 2-2, although this is not a hard-and-fast rule. Similarly, the decision time horizon changes from several years, and great uncertainty, to a more immediate time frame with less uncertainty. The uncertainty that may have existed is often removed from consideration as one moves from left to right as a result of previous decisions. For example, what fraction of cargo to inspect is a decision assumed to have a fairly long time scale, and it is followed by more targeted (and perhaps shorter-lived) decisions about *how* to inspect—does one examine manifests, use some type of detector, or physically open containers? Associated decisions resolve where to set the threshold for triggering an alarm and similar protocols. Clearly, all these levels of decision are interrelated. There is no sense in deciding on a level of inspection that there is no way to implement or that is operationally too expensive.

Some policy level trade-offs must be made in the absence of much or any historical data and rely, instead, perhaps on surveys and formal expert elicitations; it is unfortunate that often the most consequential decisions have the fewest data to support them. The paucity of historical data complicates the analysis of risks associated with different terrorism scenarios. However, there are approaches to developing other types of threat data for use in quantitative models that should be used, when appropriate, by DHS. These include, for example, elicitation of expert judgments, game theory, and Bayesian techniques. While there will be uncertainties associated with these approaches, they are nevertheless important. The shortage of historical data does not obviate the value of carefully crafted and well-documented estimates of risk, with appropriate characterization of the uncertainties.

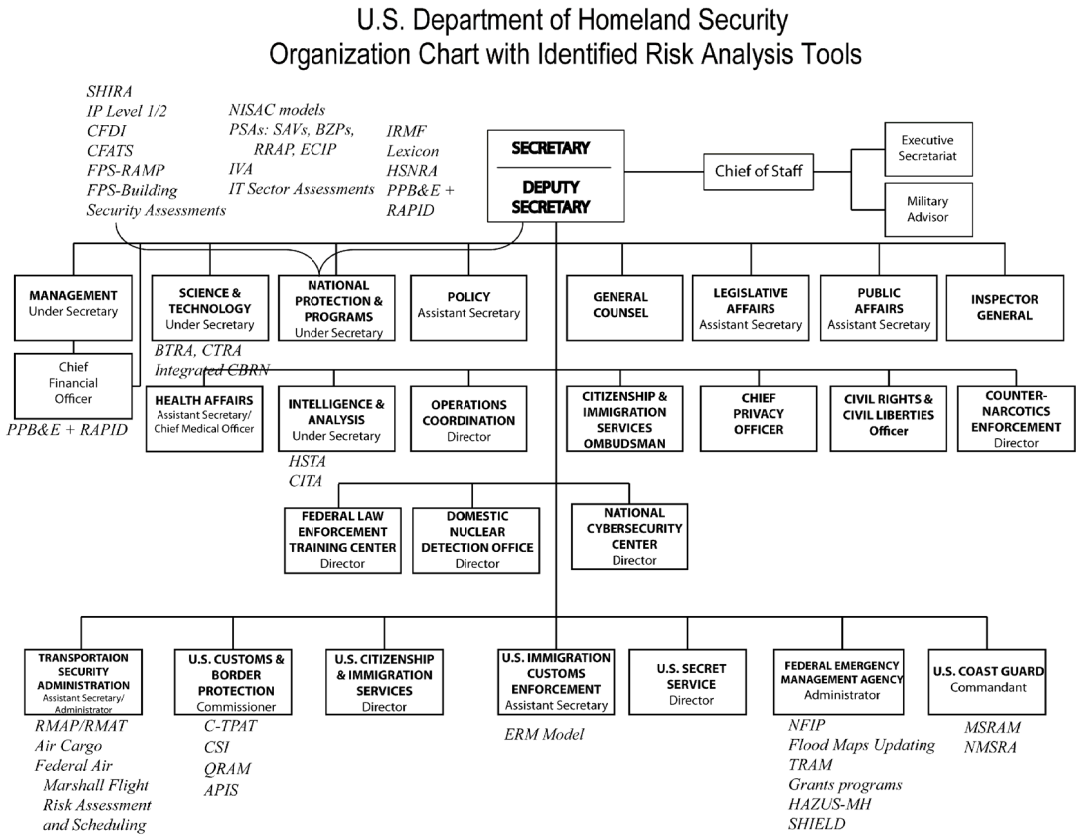

FIGURE 2-1 The DHS organizational chart (with a sample of risk models associated by unit).

TABLE 2-1 Acronym Key and Notes for Risk Models and Processes shown in Figure 2-1[a]

Acronym (from Figure 2-1)	Full Name	Notes
HITRAC*	Homeland Infrastructure Threat and Risk Analysis Center	A joint program of the Office of Infrastructure Protection (IP) and the Intelligence and Analysis Directorate (I&A)
SHIRA	Strategic Homeland Infrastructure Risk Assessment	A high-level risk assessment of infrastructure elements
IP Level 1/2	Also known as the "Level 1/Level 2" program	A risk-based process for identifying high-risk infrastructure targets
CFDI	Critical Foreign Dependencies Initiative	A process for examining supply chains to identify critical vulnerabilities
CFATS	Chemical Facility Anti-Terrorism Standards	A risk-based method for identifying which chemical facilities will be regulated by DHS
NISAC models*	Models and simulations from the National Infrastructure Simulation and Analysis Center	Most NISAC work informs consequence analyses
PSAs	Protective Security Advisors	A program that provides security consultations to owners and operators of critical infrastructure elements
SAVs	Site Assistance Visits	Evaluations performed by PSAs
BZPP	Buffer Zone Protection Program	A program that identifies, based on analyses of risk, which areas contiguous to critical infrastructure elements merit their own protection
RRAP*	Regional Resiliency Assessment Projects	Risk-based assessments of the resiliency of clusters of critical infrastructure and their buffer zones
ECIP	Enhanced Critical Infrastructure Protection Initiative	An in-progress effort to improve the method for scoring vulnerabilities of critical infrastructure and key resources
IVA	Infrastructure Vulnerability Assessment	A process under development to integrate site-specific vulnerability information with other vulnerability assessments to create a more integrated picture of vulnerabilities to guide risk assessment and management

continues next page

TABLE 2-1 Continued

Acronym (from Figure 2-1)	Full Name	Notes
RMA*	Office of Risk Management and Analysis	DHS office charged with coordination of risk analysis across the department
IRMF*	Integrated Risk Management Framework	Structure for coordination being developed by RMA and the document that guides that coordination
Lexicon	DHS risk lexicon	Defines risk analysis terms
HSNRA-QHSR	Homeland Security National Risk Assessment, Quadrennial Homeland Security Review	The QHSR, released February 2010, proposes the development of a capability to perform HSNRAs
PPBE + RAPID	Planning, Programming, Budgeting, and Execution; Risk Analysis Process for Informed Decision-Making	PPB&E is the process used in DHS's finance office to build the budget. RAPID is a tool under development to supply risk analysis to inform that process
BTRA*	Biological Threat Risk Assessment	A computationally intensive, probabilistic event-tree model for assessing bioterrorism risks
CTRA	Chemical Threat Risk Assessment	A computationally intensive, probabilistic event-tree model for assessing chemical terrorism risks
Integrated CBRN	Integrated Chemical-Biological-Radiological-Nuclear risk assessment	A computationally intensive, probabilistic event-tree model for developing an integrated assessment of the risk of terrorist attacks using biological, chemical, radiological, or nuclear weapons
HSTA	Homeland Security Threat Assessment	An I&A program to develop an understanding of threats
CITA	Critical Infrastructure Threat Assessment Division	An I&A unit that produces threat analyses for critical infrastructure and key resources
IT Sector Risk Assessment	Information Technology Sector Risk Assessment	A process to assess risks against the IT infrastructure
RMAP/RMAT	Risk Management Analysis Process/Tool	RMAT is an agent-based tool under development by Boeing and TSA to evaluate airport vulnerabilities. RMAP is the emerging process to make use of RMAT

TABLE 2-1 Continued

Acronym (from Figure 2-1)	Full Name	Notes
Air Cargo		Risk-informed method for selecting targets for screening. Not examined by this study.
Federal Air Marshalls' Flight Risk Assessment & Scheduling		Risk-informed method for selecting flights to carry an Air Marshall. Not examined by this study
C-TPAT	Customs-Trade Partnership Against Terrorism	Risk-informed process for examining security across worldwide supply chains. Not examined by this study
CSI	Container Security Initiative	CSI uses threat information and automated targeting tools to identify containers for inspection at borders. Not examined by this study.
QRAM	Quantitative risk assessment model	A general class of models used in part to set inspection levels at borders. Not examined by this study.
APIS	Advance Passenger Information System	APIS uses threat information to identify passengers who should not be allowed to travel to or leave the United States by aircraft or ship. Not examined by this study
ICE ERM Model	Immigration and Customs Enforcement Enterprise Risk Management model	A process, in the early stage of development, through which ICE plans to manage risks holistically across the entire enterprise. Not examined by this study
FPS-RAMP	Federal Protective Service-Risk Assessment Management Program	RAMP, which is in the early stage of development, is intended to be a systematic, risk-based means of capturing and evaluating facility information. Not examined by this study
FPS-Building Security Assessments		FPS security assessments of federal buildings
NFIP*	National Flood Insurance Program	A risk-based federal insurance program
Flood Maps Updating		Floodplain maps for the United States underpin the NFIP, and ongoing improvements improve the precision of risk analysis underlying the NFIP

continues next page

TABLE 2-1 Continued

Acronym (from Figure 2-1)	Full Name	Notes
TRAM*	Terrorism Risk Assessment and Management	A computer-assisted tool to analyze risks primarily in the transportation sector.
Grants programs*		FEMA allocates grants to first responders and others through a variety of programs. Some allocations are based on formula, whereas others are based on coarse assessments of risk
HAZUS-MH	HAZards U.S.—Multi-hazard	A software tool that uses databases of physical infrastructure to analyze potential losses from floods, hurricane winds, and earthquakes
SHIELD	Strategic Hazards Identification and Evaluation for Leadership Decisions	A scenario-based regional risk analysis for the National Capital Region
MSRAM	Maritime Security Risk Analysis Model	A computer-assisted tool to analyze risks primarily in the maritime sector.
NMSRA	National Maritime Strategic Risk Assessment	A process used by the Coast Guard to identify risks to achieving its performance goals and identifying mitigation options. Not examined by this study

[a]Except as noted, the study committee examined each of these. Starred terms in the first column are discussed in some depth in this report.

Span of Risk Informed Decisions Considered by DHS

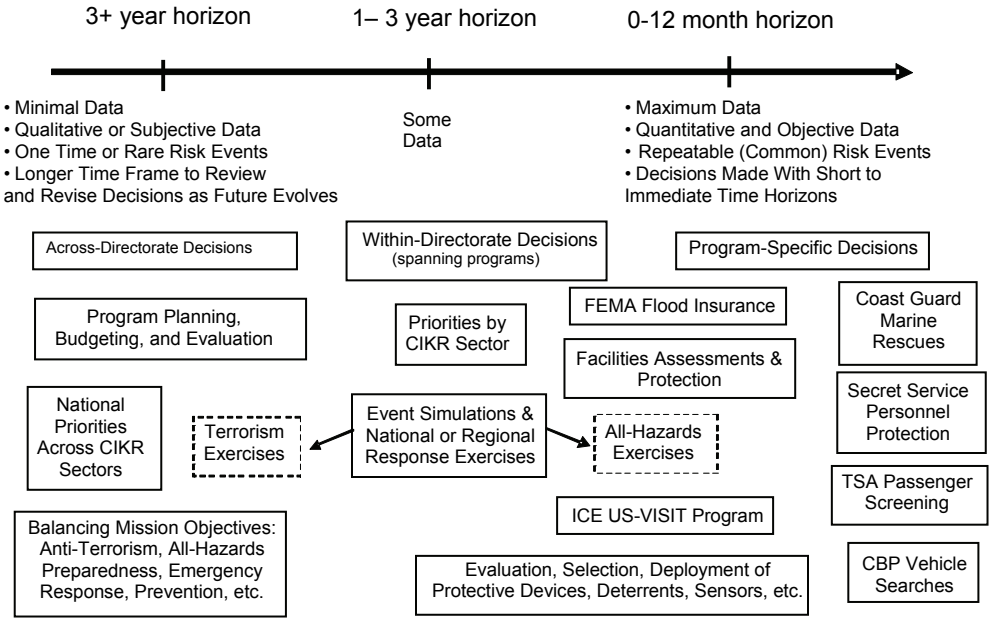

FIGURE 2-2 Types of risk-informed decisions that DHS faces (in boxes) arrayed roughly according to the decision-making horizon they inform.

Once policy decisions have been made, strategies can be aligned to support each policy tenet.[1] For example, it may be that DHS leadership makes the policy decision to apply equal resources to counterterrorism and natural hazards preparedness. Once those allocations are made, strategic decisions must be made about how to apportion resources to address particular natural hazards and particular terrorism threats. Note that this approach implicitly avoids the necessity of comparing the risks of for example, floods to the risks of nuclear attacks, because a policy decision has already been made to divide resources equally between natural hazards and terrorism. Clearly there are other methods to parse the policy questions, but this illustrates how uncertainly can be removed at the policy level, thus simplifying strategic decisions.

[1] In a perfect world, policy decisions would be predicated on the strategic, tactical, and operational decisions that they imply, and the serial process implied by this paragraph would be replaced with a process that considers the entire range of intertwined decisions as a whole.

REVIEW OF CURRENT PRACTICES OF RISK ANALYSIS WITHIN DHS

The remainder of this chapter summarizes the current practices of risk analysis within DHS for six illustrative methods: (1) risk analysis for natural hazards; (2) threat, vulnerability, and consequence analyses performed for protection of Critical Infrastructure and Key Resources (CIKR) protection; (3) risk models used to underpin those DHS grant programs for which allocations are based on risk; (4) the Terrorism Risk Assessment and Management (TRAM) tool; (5) the Biological Threat Risk Assessment (BTRA) methodology; and (6) the Integrated Risk Management Framework (IRMF). The committee does not attempt to document the many other risk models and practices within DHS. Risk analysis for natural disasters is discussed first because it is the most mature of these processes.

Risk Analyses for Natural Hazards

DHS's natural hazards preparedness mission is addressed principally within the Federal Emergency Management Agency (FEMA). With minor exceptions (e.g., the U.S. Coast Guard), no other DHS component has a significant natural hazard mission. In natural hazards, FEMA is concerned with a variety of threats, such as tornadoes, hurricanes, earthquakes, floods, wildfires, droughts, volcanoes, and tsunamis.

FEMA's authority for flood hazard resides largely in the National Flood Insurance Program, (NFIP), which represents a substantial responsibility. The NFIP is administered by a core staff of employees with support from contractors (i.e., consulting firms with expertise in hydrology, hydraulics, and floodplain studies). FEMA's role with respect to other natural hazards deals principally with mitigation and response rather than risk analysis and thus is not addressed by this report. For example, the U.S. Geological Survey (USGS) has the primary responsibility for assessing earthquake hazards, while FEMA deals with developing emergency plans for responding to earthquakes and recovering from their effects. Jointly, the USGS and FEMA help inform planning for building codes so as to reduce vulnerabilities and strengthen the nation's resilience to such hazards. Risk analysis often informs this mitigation and response planning.

FEMA's risk analysis related to flooding serves as the basis for the creation of NFIP flood insurance rate maps and the setting of flood insurance rates. The risk assessments involve statistical analyses of large historical datasets, obtained primarily from USGS stream gages, and hydraulic computations that produce flood-frequency relations, water surface profiles, and maps showing flood zone delineations. In the context of this program, information on regional hydrology, statistical methods, river hydraulics, and mapping is constantly being improved

(largely because these are of broad interest and application within the larger water resources enterprise). FEMA's risk analyses in support of the NFIP are based on generally good data and mature, well-understood science. Importantly, the analysis of natural hazards and their risks generally proceeds from empirical data. Hundreds of Ph.D. theses and natural events have led to many ways of validating the models for natural hazard risks. For example, one can compare the actual frequency of floods occurring in various flood zones after a flood map has been developed for a community. Over many years, the NFIP has been the subject of much scrutiny and occasional external assessments and reviews by associations, consultants, and others, including the National Research Council (NRC). Recent reports by the NRC (2007a, 2009) provide a good current assessment and recommendations for improving flood risk assessment.

Analyses in Support of the Protection of Critical Infrastructure

One of the primary new responsibilities assigned to DHS-IP (2009) when it was established was to develop the National Infrastructure Protection Plan (NIPP), which

> provides the coordinated approach that is used to establish national priorities, goals, and requirements for CIKR protection so that Federal resources are applied in the most effective and efficient manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified under the authority of Homeland Security Presidential Directive 7 (HSPD-7), and addresses the physical, cyber, and human considerations required for effective implementation of protective programs and resiliency strategies. [Available online at *http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf.*]

DHS's Office of Infrastructure Protection (IP) has the mandate to produce threat, vulnerability, and consequence analyses to inform priorities for strengthening CIKR assets.

Table 2-2 lists the 18 CIKR sectors and the federal agency or agencies that have the lead responsibility for managing the associated risks. DHS has lead responsibility for 11 of the sectors, and it is to provide supporting tools and analysis for the others, working with the Department of Energy to protect the electrical grid, the Department of Health and Human Services on public health, and the Environmental Protection Agency with respect to the nation's water supply. DHS works with these agencies to develop sector-specific plans and risk assessments. Maintaining a strong interface between DHS and other federal agencies—in order to share information, tools, and insight—is key to solidifying our nation's security in those sectors for which responsibility is shared.

TABLE 2-2 CIKR Sectors and Federal Agencies with Lead Responsibility for Managing the Associated Risks

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture Department of Health and Human Services	Agriculture and food
Department of Defense	Defense industrial base
Department of Energy	Energy
Department of Health and Human Services	Health care and public health
Department of the Interior	National monuments and icons
Department of the Treasury	Banking and finance
Environmental Protection Agency	Water
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial facilities Critical manufacturing Dams Emergency services Nuclear reactors, materials, and waste
Office of Cybersecurity and Communications	Information technology Communications
Transportation Security Administration	Postal and shipping
Transportation Security Administration, U.S. Coast Guard	Transportation systems
Immigration and Customs Enforcement, Federal Protection Services	Government facilities

SOURCE: DHS-IP (2009, p. 3). Available online at *http://www.dhs.gov/xlibrary/assets/NIPP_ Plan.pdf*. Accessed November 20, 2009.

Threat analyses are facilitated by the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) program, which is a joint program of IP and DHS's Office of Intelligence & Analysis (I&A). The latter is DHS's interface with the intelligence community and provides expertise and threat information. Many of the I&A professional staff have been hired from other intelligence agencies, and they provide DHS with a formal and informal intelligence network.

I&A's Critical Infrastructure Threat Assessment (CITA) division, working with Argonne National Laboratory, established the process to provide threat information for the 18 CIKR sectors as well as for other DHS needs. CITA determines threat through structured subject matter elicitation. Some of the subject matter experts (SMEs) are staff from within I&A; others are enlisted from elsewhere in the intelligence community. Attack scenarios are developed to represent how SMEs would expect different sorts of terrorist groups (e.g., domestic terrorist, sophisticated Islamic terrorists), to go about attacking particular CIKR assets. The CIKR sectors and I&A work jointly to develop the scenarios. I&A's inputs include analytic papers and reports on threats affecting particular states and urban areas. About 25 attack scenarios are generated per sector. The same scenarios are used year after year with modification as needed as more is learned about tactics and techniques. The mix of SMEs often changes, which might limit the consistency of the estimates but also serves to introduce fresh thinking. During elicitation, the SMEs work through a structured process to score the likelihood of the various threats against each type of CIKR asset. Infrastructure vulnerability experts also can be asked to participate. The committee did not examine the elicitation process in detail.

When developing threat estimates with the involvement of uncleared experts, the SMEs are given generic attack scenarios against generic infrastructure assets. Generic attack scenarios allow for the moving of classified information to the unclassified level and also some consistency in the variables described across scenarios. The attack scenarios are developed by intelligence analysts drawing on experts, previous attacks, and reporting. Each scenario includes descriptions of the mode of attack (e.g., a vehicle-borne improvised explosive device), how the terrorist gains access, the target, the terrorist goal, and the geographical regional or location. The process includes training for the SMEs on how to provide expert judgment with the least chance for bias. Such training, for both SMEs and those who perform the elicitation, is critical because it is well known that biases can be introduced in expert elicitation, and there are established methods for lessening this risk.

One major HITRAC product is an annual distillation, based on data from states and from CIKR sector councils, to identify lists of high-risk CIKR assets. These lists are used to guide resource allocation. HITRAC does not rely solely on quantitative analysis; one of its sources of information is red-team exercises, using staff with backgrounds in military special forces to brainstorm CIKR vulnerabilities. Another HITRAC risk product is the Strategic Homeland Infrastructure Risk Assessment (SHIRA). According to the National Infrastructure

Protection Plan of 2009,

> [T]he SHIRA involves an annual collaborative process conducted in coordination with interested members of the CIKR protection community to assess and analyze the risks to the Nation's infrastructure from terrorism, as well as natural and manmade hazards. The information derived through the SHIRA process feeds a number of analytic products, including the National Risk Profile, the foundation of the National CIKR Protection Annual Report, as well as individual Sector Risk Profiles. [DHS-IP, 2009, p. 33]

Risk-Informed Grants Programs

Another major DHS responsibility is issuing grants to help build homeland security capabilities at the state and local levels. Most such money is distributed through FEMA grants, of which there are numerous kinds, some with histories dating to the establishment of FEMA in the mid-1970s. In 2008, FEMA awarded more than 6,000 homeland security grants totaling over $7 billion. Five of these programs, covering more than half of FEMA's grant money—the State Homeland Security Program (SHSP), the Urban Areas Security Initiative (UASI), the Port Security Grant Program (PSGP), the Transit Security Grant Program (TSGP), and the Interoperable Emergency Communications Grant Program (IECGP)—incorporate some form of risk analysis in support of planning and decision making. Two others inherit some risk-based inputs produced by other DHS entities—the Buffer Zone Protection Program, which allocates grants to jurisdictions near critical infrastructure if they are exposed to risk above a certain level as ascertained by IP, and the Operation Stonegarden Grant Program, which provides funding to localities near sections of the U.S. border that have been identified as high risk by Customs and Border Protection. All other FEMA grants are distributed according to formula.

Even for the grant programs that are risk-informed, FEMA has to operate within constraints that are not based on risk. For example, Congress has defined which entities are eligible to apply for grants and, for the program of grants to states, it has specified that every state will be awarded at least a minimum amount of funding. Congress stipulated that risk was to be evaluated as a function of threat, vulnerability, and consequence, and it also stipulated that consequence should be a function of economic effects, presence of military facilities, population, and presence of critical infrastructure or key resources (the 9/11 Act of 2007 (P.L. 110-53), Sec. 2007). However, FEMA is free to create the formula by which it estimates consequences, and it has also set vulnerability equal to 1.0, effectively removing it from consideration. The latter move is in part driven by the difficulty of performing vulnerability analyses for all the entities that might apply to the grants programs. FEMA does not have the staff to do that, and the grant allocation time line set by Congress is too ambitious to allow

detailed vulnerability analyses.

DHS also has latitude to define "threat." In the past, it defined threat for grant making as consisting solely of the threat from foreign terrorist groups or from groups that are inspired by foreign terrorists. That definition means that the threat from narcoterrorism, domestic terrorism, or other such sources was not considered. This decision is being reviewed by the DHS Secretary.

For most grant allocation programs, FEMA weights the threat as contributing 20 percent to overall risk and consequence as contributing 80 percent. For some programs that serve multihazard preparedness, those weights have been adjusted to 10 percent and 90 percent, respectively, in order to lessen the effect that the threat of terrorism has on the prioritizations. Because threat has a small effect on FEMA's risk analysis, and population is the dominant contributor to the consequence term, the risk analysis formula used for grant making can be construed as one that, to a first approximation, merely uses population as a surrogate for risk. FEMA does not have the time or staff to perform more detailed or specialized consequence modeling, and the committee was told that this coarse approximation is relatively acceptable to the entities supported by the grants programs. It is not clear whether FEMA has ever performed a sensitivity analysis of the weightings involved in these grant allocation formulas or evaluated the ramifications of the (apparently ad hoc) choices of weightings and parameters in the consequence formulas. Such a step would improve the transparency of these crude risk models.

The FEMA grants program is working on an initiative called Cost-to-Capability (C2C). This was begun to emulate the way the Department of Defense analyzes complex processes and drives toward optimal progress. The objective is to identify the information needed to manage homeland security and preparedness grant programs. The C2C model replaces "vulnerability" with "capability," in a sense replacing a measure of gaps with a measure of hardness against threats. A Target Capabilities List (TCL) identifies 37 capabilities among four core mission areas of prevention, protection, response, and recovery. The TCL includes capabilities ranging from intelligence analysis and production to structural damage assessment. The critical element of C2C is to identify the importance of such capabilities to each of the 15 national planning scenarios used to develop target capabilities. This intends to open up the possibility of aggregating capabilities to create a macro measure of national "hardness" against homeland security hazards. The C2C initiative is still in a conceptual stage and had been heavily criticized in congressional hearings, but it appears to be a reasonable platform by which the homeland security community can begin charting a better path toward preparedness. A contractor is creating software, now ready for pilot testing, that will allow DHS grantees to perform self-assessments of the value of their preparedness projects, create multiple investment portfolios and rank them, and track portfolio performance.

Risk Analysis in TRAM

The Terrorism Risk Assessment and Management (TRAM) toolkit is a mature software-based method for performing terrorism-related relative risk analysis primarily in the transportation sector. It helps owner-operators and other SMEs identify their most critical assets, the threats and likelihood of certain classes of attacks against those assets, the vulnerability of those assets to attack, the likelihood that a given attack scenario would succeed, and the ultimate impacts of the total loss of the assets on the agency's mission. TRAM also helps to identify options for risk management and assists with cost-benefit analyses.

Overall, TRAM works through six steps to arrive at a risk assessment:

1. Criticality assessment
2. Threat assessment
3. Vulnerability assessment
4. Response and recovery capabilities assessment
5. Impact assessment
6. Risk assessment

Working through the process, the first step in the overall TRAM risk assessment is evaluation of the criticality of each of the agency's assets to the mission. This includes a quantification and comparison of assets to identify those that are most critical. In making the determination, factors that the agency most wishes to guard against are identified: for example, loss of life or serious injury; the ability of the agency to communicate and move people effectively; negative impacts on the livelihood, resources, or wealth of individuals and businesses in the area, state, region, or country; or replacement cost of critical assets of the agency

The TRAM process then guides SMEs through a threat assessment. A potential list of specific types of threats (e.g., attack using small conventional explosives, large conventional explosives, chemical agents, a radiological weapon, or biological agents) is considered, and for each the SMEs are asked to estimate the likelihood of the specific attack type occurring against the agency's critical assets. The analysis is also informed by general considerations of whether a terrorist group would be capable of such an attack and motivated to carry it out on the asset(s) in question.

Steps 3 to 5—vulnerability assessment, response and recovery capabilities assessment, and impact assessment—are similarly effected through expert elicitation, drawing largely on the knowledge and experience of agency security experts, engineers, and other experienced professional staff with a strong under-

standing of their assets and operations.[2] The vulnerability assessment component evaluates the vulnerability of the identified critical assets to the specific threat scenarios. In relation to response, the TRAM process calls for local emergency response organizations to weigh in by performing self-assessments of their ability to support the mission of the agency being reviewed. Capabilities, gaps, and shortfalls with respect to aspects such as staffing, training, equipment and systems, planning, exercises, and organizational structure are considered relevant. The recovery assessment reviews the agency's own functions and capabilities for managing aspects of recovery and business continuity. That assessment addresses elements such as plans and procedures, alternate facilities, operational capacity, communications, records and databases, and training and exercises. Impact assessment is designed to lead to the calculation of consequence measures for each particular threat scenario. This part of the process adds a sensitivity component to the analysis by taking into account not just the worst-case scenario in which there is a total loss of the critical asset, but also less extreme results. At step 6, risk assessment, the TRAM software is operated in batch mode—the parameters for a particular analysis are specified up front and the model is run offline. A complete set of scenarios, risk results, and a relative risk diagram are the outputs. The two-dimensional risk diagram shows a comparison of risk between scenarios based on their overall ratings of likelihood and consequence. Work is under way to expand TRAM to multiple hazards beyond terrorism. These might include human-initiated hazards such as sabotage and vandalism; technological hazards such as failure in structures, equipment, or operations; and natural hazards such as hurricanes, earthquakes, and blizzards.

Biological Threat Risk Assessment

The Biological Threat Risk Assessment tool is a computer-based probabilistic risk analysis (PRA), using a 17-stage event tree, to assess the risk associated with the intentional release of each of 29 biological agents. An NRC committee reviewed the method used to produce the 2006 biological threat risk assessment and found that the basic approach was problematic (NRC, 2008), as explained in Chapter 4. While some changes have been made and more are slated for the future, the same general approach is apparently still in use for assessments of biological threats, chemical threats, and DHS's integrated chemical, biological, radiological, and nuclear (iCBRN) risks and, in particular, was used to produce biological risk assessments released in January, 2008, and January, 2010. The best description of the BTRA method is found in Chapter 3 of the NRC review.

[2] The TRAM toolkit contains the following note regarding expert elicitation: "The impact assessment requires a multidisciplinary team of experts with knowledge of an asset's structural strengths and deficiencies, as well as individuals with a working knowledge of methodologies for assessing WMD damage."

It describes the method as follows (NRC, 2008, p. 22):

> The process that produced the estimates in the BTRA of 2006 consists of two loosely coupled analyses: (1) a PRA event-tree evaluation and (2) a consequence analysis.
>
> A PRA event tree represents a sequence of random variables, called events, or nodes. Each random-event branching node is followed by the possible random-variable realizations, called outcomes, or arcs, with each arc leading from the branching, predecessor node, to the next, successor-event node (and it can be said without ambiguity that the predecessor event selects this outcome, or, equivalently, selects the successor event). With the exception of the first event, or root node, each event is connected by exactly one outcome of a preceding event …. The path from the root to a particular leaf is called a scenario ….
>
> The 17 stages modeled in BTRA are as follows:
>
> - Frequency of initiation by terrorist group
> - Target selection
> - Bioagent selection
> - Mode of dissemination (also determines wet or dry dispersal form)
> - Mode of agent acquisition
> - Interdiction during acquisition
> - Location of production and processing
> - Mode of agent production
> - Preprocessing and concentration
> - Drying and processing
> - Additives
> - Interdiction during production and processing
> - Mode of transport and storage
> - Interdiction during transport and storage
> - Interdiction during attack
> - Potential for multiple attacks
> - Event detection

The evaluation of consequences is performed separately, not as part of the event tree (NRC 2008, p. 27):

> Consequence models characterize the probability distribution of consequences for each scenario. The BTRA employs a mass-release model that assesses the production of each bioagent, beginning with time to grow and produce, preprocess and concentrate, dry, store and transport, and dispense. The net result is a biological agent dose that is input to a consequence model to assess casualties. One equation from the model is produced here to give a flavor of the computations.

$$MR = MT \times QF_1 \times QF_2 \times QF_3 \times QF_4 \times QF_5$$

where *MR* is bioagent mass release, *MT* is target mass, and QF_i are factors to explain production, processing, storage, and so on and are random variables conditioned on the scenario whose consequences are being evaluated.

The complete model computes, for an attack with a given agent on a given target, how much agent has been used, how efficiently it has been dispersed (and, for an infectious agent, how far it spreads in the target population), and the potential effects of mitigation efforts. For the BTRA of 2006, all of these factors were assigned values by eliciting opinions of subject-matter experts in the form of subjective discrete probability distributions of likely outcomes, and by some application of information on the spread of infectious agent, atmospheric dispersion, and so on.

The BTRA consequence analysis is qualitatively different from its event-tree analysis. Subject-matter expert opinions are developed much like case studies, and there is less clear dependence on specific events leading to each consequence. Thus, each consequence distribution should be viewed as being dependent on *every* event leading to its outcome …. A Monte Carlo simulation of 1,000 samples was used to estimate each consequence distribution in the BTRA of 2006.

Integrated Risk Management Framework

Recognizing the need for coordinated national-level risk management, on April 1, 2007, DHS created the Office of Risk Management and Analysis (RMA) within the National Protection and Programs Directorate. Serving as DHS's executive agent in charge of national-level risk analysis standards and metrics, RMA has the broad responsibility to synchronize, integrate, and coordinate risk management and risk analysis approaches throughout DHS (*http://www.dhs.gov/xabout/structure/gc_1185203978952.shtm*). RMA is leading DHS's effort to establish a common language and an integrated framework as a general structure for risk analysis and coordination across the complex DHS enterprise.

RMA's development of the IRMF and supporting elements generally follows implementation of Enterprise Risk Management (ERM) in the private sector, most closely aligning with ERM practices in nonfinancial services companies. A brief overview of ERM is provided next to better explain the parallels between ERM as implemented in the private sector and IRMF as developed and implemented by RMA.

Enterprise Risk Management was sparked by concerns in the late 1990s about the "Y2K problem," the risk that legacy software would fail when presented with dates beginning with "20" rather than "19." In order for a firm to characterize its risk exposure to this problem, it was necessary to develop processes that enabled top management to identify not only information technology risks within discrete business units, but also those risks that arise or increase due

to interactions, synergies, or competition among business units. Building on a base of data analysis and risk modeling, ERM also relies on good processes for the establishment of strong management processes, common terminology and understanding, and high-level governance. ERM is risk management performed and managed across an entire institution (across silos) in a consistent manner wherever possible. This requires some entity with a top-level view of the organization to establish processes for governing risk management across the enterprise, coordinating risk management processes across the enterprise, and working to establish a risk-aware culture. ERM systems do not "own" unit-specific risk management, but they impose some consistency so that those risk management practices are synergistic and any data collected are commensurate. The latter allows for more rational management and resourcing across units. ERM systems also provide steps to aggregate risk analyses and risk management processes up to the top levels of the organization so as to obtain an integrated view of all risks. When viewed through the lens of aggregation, some risks that are of low probability for any given unit are seen to have a medium or high probability of occurring *somewhere* in the enterprise, and some risks that are of low consequence to any given unit can have a high consequence if they affect multiple units simultaneously.

More generally, ERM provides an understanding of potential barriers that must be recognized and managed to achieve program and strategic objectives. It also informs decision makers of corporate challenges and mitigation strategies, and it provides a basis for risk-based executive-level decisions. A comprehensive ERM framework strengthens leaders' ability to better anticipate internal and external risks, and it allows risk to be addressed early enough to preserve a full range of mitigation options, and plan responses and generally to reduce surprises and their associated costs.

By and large, RMA appears to be trying to establish the elements commonly accepted as fundamental to ERM: governance, processes, and culture.

- Governance includes the framework for strategic and analysis-driven decision making, high-level review and reporting, and ongoing strategic assessment of policies, procedures, and processes.
- Processes include those for identification, assessment, monitoring, and resolution of risks at all levels of the enterprise.
- Culture includes language, values, and behavior.

An interim draft of the Integrated Risk Management Framework was released in January 2009. The IRMF is intended to provide doctrine and guidelines that enable consistent risk management throughout DHS in order to inform enterprise-level decisions. It is also meant to be of value to risk management at the component level that informs decisions within those components. The objectives of the IRMF are to "[i]mprove the capability for DHS components to utilize risk management to support their missions, while creating mechanisms

for aggregating and using component-level risk information across the Department, [to support the] strategic-level decision-making ability of DHS by enabling development of strategic-level analysis and management of homeland security risks, [and to] institutionalize a risk management culture within DHS."[3] "The IRMF outlines a vision, objectives, principles and a process for integrated risk management within DHS, and identifies how the Department will achieve integrated risk management by developing and maturing governance, processes, training, and accountability methods" (DHS-RSC, 2009, p. 1-2). In addition, the IRMF is meant to help institutionalize a risk management culture within DHS (DHS-RSC, 2009, p. 12). The IRMF is gradually being supplemented with analytical guidelines that serve as primers on specific practices of risk management within DHS. Two recent draft guidelines that are adjuncts to the IRMF have addressed risk communication to decision makers and development of scenarios.

Other RMA activities to support IRMF (and, more generally, achieve the vision of ERM) include cataloging of risk models and processes in use across DHS, formation and coordination of a Risk Steering Committee (RSC), development of a risk lexicon, and work on the RAPID process (Risk Analysis Process for Informed Decision-Making) to link risk analysis to internal budgeting.

RMA has catalogued dozens of risk models and processes across DHS (DHS-RMA, 2009). A side benefit of this effort was that it presumably helped to establish an informal network of relationships and technical capabilities among at least some of the component units. Through that network, it is hoped that training, education, outreach, and success stories can migrate from the more risk-mature component units to those with less mature risk management practices.

Additionally, RMA is working to foster a coordinated, collaborative approach to risk-informed decision making by facilitating engagement and information sharing of risk expertise across components of DHS. It does this through meetings of the RSC, which is intended to promote consistent and comparable implementations of risk management across the department. The Under Secretary for National Protection and Programs chairs the RSC, whose members consist of component heads and various key personnel responsible for department-wide risk management efforts.

The DHS Risk Lexicon was released in September 2008 (DHS-RSC, 2008). It was developed by a working group of the RSC, which collected, catalogued, analyzed, vetted, and disseminated risk-related words and terms used throughout DHS.

The RAPID process is being developed to meet the strategic risk information requirements of DHS's Planning, Programming, Budgeting, and Execution (PPBE) system. It is meant to assess how DHS programs can work together to reduce or manage anticipated risks in attaining Departmental goals and objec-

[3] Quotes taken from Tina Gabbrielli, RMA director, presentation to the committee, May 21-22, 2009, Washington, D.C.

tives, ensure that decisions about future resource allocations are informed by programs' potential for risk reduction, and support key DHS decision makers with a standardized assessment process to answer the basic risk management questions, How effectively are DHS programs helping to reduce risk? and What should we be doing next?[4] RAPID, which is still at the prototype stage, consists of the following seven steps:

- Select a representative sample of scenarios.
- Build "attack paths" for each of the terrorist scenarios, turning the scenarios into a sequence of major activities.
- For each activity in the attack path, use expert elicitation to assign probability estimates for (a) the probability that the terrorist chooses or accomplishes the activity, (b) the effectiveness of DHS programs in stopping the activity, and (c) the overall likelihood for the scenario.
- Estimate the risk of a successful attack in terms of the consequences (lives lost, direct and indirect economic effects).
- For each DHS program, calculate the risk reduction based on the threat probabilities and that program staff's judgment of the program effectiveness.
- Estimate the effectiveness of national (non-DHS) capabilities.
- Assess risk reduction alternatives.

CONCLUDING OBSERVATION

During the course of this study, DHS was very helpful in setting up briefings and site visits. However, the committee's review of DHS risk analysis was hampered by the absence of documentation of methods and processes. This gap will necessarily hinder internal communication within DHS and any attempt at internal or external review. The risk analysis processes for infrastructure protection, the grants program, and the IRMF were documented mostly through presentations. With the exception of NISAC work, the committee was not told about or shown any document explaining the mathematics of the risk modeling or any expository write-up that could help a newcomer understand exactly how the risk analyses are conducted. For example, there are apparently very detailed checklists to guide CIKR vulnerability assessments, which the committee did not need to examine, but the committee was not given any clear documentation of how the resulting inputs were used in risk analysis. The committee was told in general terms how the grants program calculates risk, but the people with whom the committee interacted did not know the exact formula and could not

[4] Tina Gabbrielli, RMA director, presentation to the committee. November 24-25, 2008, Washington, D.C.

point to a document. The committee did get to see emerging documentation about some aspects of IRMF, but important components such as the RAPID process for linking risk to budgets were presented only through charts.

The risk assessments done by FEMA to underpin the National Flood Insurance Program are better documented, in part because of their long history, perhaps because they are linked to an academic community. The NRC committee that reviewed the BTRA methodology had difficulty understanding the mathematical model and its instantiation in software, and noted in its report that the classified description produced by DHS lacked essential details. (The current study did not re-examine those materials to determine whether documentation had improved.) The TRAM model is fairly well described in an "official-use-only" document, the Methodology Description dated May 13, 2009, but there is no open-source description.

Because of this lack of documentation, the committee has had to infer details about DHS risk modeling in developing this chapter.

3
Challenges to Risk Analysis for Homeland Security

This chapter discusses challenges facing the Department of Homeland Security (DHS) in the two domains of natural hazard and terrorism risk analysis. The analysis of natural hazard risks is reasonably mature and is derived from both historical data and physics-based modeling. The analysis of terrorism risk is less mature, and it lacks both historical validating data and sociological theory on which to base quantitative models. A summary of these challenges is presented in Box 3-2 at the end of the chapter.

COMPARISON OF RISK ASSESSMENT OF NATURAL HAZARDS AND OF TERRORISM

Compared to risk analysis for countering terrorism, the analysis of natural hazard risks is well understood. For natural hazards there typically exist large historical datasets—although climate change, urbanization, evolution in the constructed environment, and so on can undercut the usefulness of those data—and a partial understanding of the physical processes involved. There are standard statistical techniques for these problems and decades of validation. There exists an understanding of model limitations, uncertainties, and the applicability of risk methodology to policy-relevant questions.[1] For example, social consequences of natural hazards are poorly understood, but research is under way to close the gap.[2] To a large extent, risk analysis methods for natural hazards reflect the principles of good practice embodied in National Research Council (NRC) reports on risk analysis and management in federal agencies (e.g., NRC, 1983).

This is not to say that the risk analyses are always straightforward. For some rare yet highly consequential events, such as compounding cascading hazards, the analysis of some natural hazard risk can become very challenging because historical data are inadequate and/or minor changes in assumed conditions can lead to orders-of-magnitude differences in risk (see Box 3-1).

[1] See, for example, Kunreuther and Michel-Kerjan (2009) and the references contained therein.
[2] Heinz Center (2000) provides a glimpse at some recent work.

BOX 3-1
Cascading Natural Hazard Risk Can Pose Analysis Problems as Challenging as those Associated with Terrorist Risk: The Case of the Sacramento-San Joaquin Bay Delta

The Sacramento-San Joaquin Bay Delta lies at the confluence of the Sacramento and San Joaquin rivers east of San Francisco. It comprises a low-lying agricultural district some 100 km by 50 km in extent, through which flows most of the runoff of the western slopes of the Sierra Nevada range. Passing through the delta, the Sierra runoff flows into the brackish San Francisco Bay and finally to the Pacific. The delta hosts some 1,800 km of levees and sloughs (the local term for canals), constructed mostly in the late nineteenth century by immigrant farmers, that are extremely fragile and create a system of below sea-level islands and wetlands.

The peat soils of the delta make the region among the most fertile agricultural areas in the world, contributing billions of dollars annually to the nation's economy. The delta also hosts the intake forebays for the California Aqueduct, carrying 60 percent of the fresh water supply for the desert-like Los Angeles region. Without the fresh water originating from the delta, Southern California would face a desperate potable water supply situation.

The delta also lies alongside the San Andreas Fault belt and is potentially subject to large peak ground accelerations should earthquakes occur along the eastern side of that belt. This natural event, which is not improbable compared to many natural hazards, would likely breach many kilometers of fragile levees; foster rapid saltwater intrusion into the delta from Suisun Bay, the easternmost extension of San Francisco Bay; and potentially compromise the quality of water entering the aqueduct. If that intrusion were sufficiently saline, a shutdown of the intakes would be necessary.

Were this calamity to happen after the spring melt in the Sierras, it could be nine months before water transfer to Los Angeles resumed. The economic and social impact of this cascading natural event would be unprecedented. Being unprecedented, it is not an event for which there are adequate historical data from which to assess risk. It is a low-probability, high-consequence risk in the natural domain, and analyzing the risk shares many features with risk analysis for counterterrorism.

In contrast, for risk assessment of terrorism threats, particularly with respect to exceedingly rare or never-observed events, the historical record is essentially nonexistent, and there is poor understanding of the sociological forces from which to develop assessment techniques. Because of the presence of a thinking (intelligent) adversary, there is an inherent dependence among the three terms, threats, vulnerabilities, and consequences (T, V, and C), and threat is difficult to express as a simple probability. An intelligent adversary will exploit opportunities where vulnerabilities and consequences are high; thus, probabilities of the threats change as we take actions to harden targets or protect the public. This

substantially complicates the risk analysis. Where threats, vulnerabilities, and consequences are not independent, risk analysis must estimate a joint probability of the correlated T, V, and C terms, substantially complicating the estimation of risk and its uncertainty. In this case risk can be evaluated as Risk = $f(T,V,C)$ but cannot be evaluated as the simpler product Risk = $T \times V \times C$.

Vulnerability studies for natural hazards are, in principle, little different from those used for terrorism risks. In the natural hazards case, vulnerability studies deal with the effects of wind, water, fire, or ground shaking, et cetera, on the built environment. In the terrorism case, the vulnerability studies deal with the effects of blast, vehicle impacts, et cetera. In both cases, the techniques of vulnerability evaluation are well understood.

The approach to risk management for some natural hazards might hold lessons for terrorism risk analysis. For example, our ability to define the threat from earthquakes has largely resisted the best efforts of scientists: we can estimate their likelihoods, based on historic records, but we cannot find signals that allow us to predict when and where one will actually strike. Therefore, risk management has focused more on reducing vulnerabilities and increasing resilience. Improvements to resilience increasingly leverage knowledge from the social sciences and include public communications efforts. As more is learned about methods to increase resilience, dual benefits might accrue.

A notable contrast between risk analysis for natural hazards and for counterterrorism is that public perception of the consequences is distorted. One telling example is that during the same year as the Oklahoma City Federal Building bombing (1995) in which 168 people perished, approximately 600 people died in a five-day period in Chicago due to unseasonable heat. Many Americans can remember where they were at the time of the Murrah Building bombing, but few even recall the deaths in Chicago.

RISK ANALYSIS FOR COUNTERTERRORISM IS INHERENTLY MORE DIFFICULT THAN RISK ANALYSIS FOR NATURAL HAZARDS

Risk analysis for natural hazards is based on a foundation of data. For terrorism risk analysis, neither threats nor consequences are well characterized by data. Risk analysis for terrorism involves an open rather than a closed system (Turner and Pidgeon, 1997): virtually anyone can be a participant (ranging from intentionally malevolent actors, to bystanders who may respond in ways that make a situation either better or worse), and parts of the system can be used in ways that are radically different from those for which they were designed (e.g., aircraft as weapons, rather than means of transportation). Also, terrorism, unlike natural disasters, involves intentional actors. Not only are many terrorist threats low-likelihood events, but their frequency is evolving rapidly over time, as terrorists observe and respond to defenses and to changing political conditions.

Thus, it will rarely be possible to develop statistically valid estimates of attack frequencies (threat) or success probabilities (vulnerability) based on historical data.[3]

Data scarcity and reliability are serious issues when attempting to assign probabilities to the threat of foreign terrorism. Despite intense efforts by the intelligence community, threat data can be episodic and too general to eliminate uncertainty. While the risk models reviewed during this study assign probabilities based on attack scenarios, it is rare for intelligence reporting to outline the attacker, the target, the technique, and the timing, so pieces of information that imply something about threats have to be found and spliced together.

Challenges of Modeling Intentional Behavior

While terrorist choices may sometimes be modeled as random processes, terrorist events do not in general occurring randomly. Rather, they reflect willful human behavior. Cox (2008) has written about the limitations of viewing threat, vulnerability, and consequences as independent concepts in such circumstances. The community of risk analysts is coming to grips with what this means for risk-analysis methodology (see, for example the Biological Threat Risk Assessment [BTRA] and the NRC review of the BTRA [NRC, 2008]). Some experts believe that there is a place for traditional risk analysis (e.g., quantitative risk analysis [QRA] or probabilistic risk analysis [PRA]) when used with suitable caveats. An example might be (von Winterfeldt and O'Sullivan, 2006) where the attack scenario is constrained enough that probabilistic modeling of the threat is reasonable. Yet others believe that such methods are generally inapplicable to intentional threats and need to be replaced by game-theoretic models (e.g., Bier, 2005; Bier, et al., 2007; Brown et al., 2005, 2006**;** Zhuang and Bier, 2007).

This is a controversial area within the technical community. Fully game-theoretic methods are not yet developed for use on problems with realistic levels of complexity, and the assumptions of defender-attacker models can be open to question. However, it is also clear that traditional risk methods fail to capture important aspects of intentional attacks and may not be adequate. In particular, risk analyses that do not reflect the ability of terrorists to respond to observed defensive actions tend to overstate the effectiveness of those actions if they ignore the ability of terrorists to switch to different targets and/or attack strategies or understate their effectiveness if they ignore the possibility of deterrence.

Therefore, better methods need to be found for incorporating the intentional nature of terrorist attacks into risk analyses, even if done judgmentally or by iterating the results of the analysis to reflect terrorist responses (Dillon et al.,

[3] Some estimate of success rate can be obtained by "gaming" attacks utilizing real players and conflict simulation models. The military uses similar models for planning attacks. They are often very scenario specific, so using them broadly may be difficult.

2009; Paté-Cornell and Guikema, 2002). Further research on game-theoretic and quasi-game-theoretic methods would also be desirable.

The military has more than 60 years of experience in using such methods to model the decision processes of intelligent adversaries so as to identify reasonable worst-case scenarios that guide defensive preparations. However, determining the actions and reaction of terrorists is harder than the task of military planners facing nation-state actors. Most nation-state adversaries have tactics and techniques that are prescribed in military doctrine, and many have established procedures for attacks and defense that are written down and exercised over long periods of time. It is often feasible to glean the doctrine, tactics, and techniques from open sources and intelligence reporting. By contrast, the doctrines of terrorist groups are more variable and harder to discern. Specific attack scenarios might be selected by a small group of individuals who desire to remain hidden.

The risk analysis discipline is working through differences of opinion about how to model intelligent adversaries, in particular addressing the question of when probabilistic methods are appropriate. Some people argue that probabilistic methods *can* be extended to encompass deliberate decisions by intelligent adversaries (e.g., Garrick et al., 2004). Yet others make a strong case that probabilistic methods are inappropriate to model the decision process of an intelligent adversary choosing from among alternate attack modes (e.g., Golany et al., 2009, Parnell et al., 2010). A recent report from the Department of Defense (DoD) advisory group JASON (2009, p. 7) goes even farther, concluding that "it is simply not possible to validate (evaluate) predictive models of rare events that have not occurred, and unvalidated models cannot be relied upon …. Reliable models for ameliorating rare events will need to address smaller, well-defined, testable pieces of the larger problem."

DHS acknowledges the need to pursue incorporating techniques of adaptive behavior in its models. Some of these techniques were recommended in the NRC's BTRA review (2008). The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) program has a Risk Analysis Division tasked with following developments in risk modeling. That division's Risk Development and Modeling Branch is charged with the integration of new theories, applied research, models, and tools. It directs efforts of the National Simulation and Analysis Center (NISAC), which has some 70 to 80 models used in various simulations. Los Alamos, Sandia, and Argonne national laboratories provide direct support.

Recommendation: DHS should consider alternatives to modeling the decisions of intelligent adversaries with fixed probabilities. Models that incorporate game theory, attacker-defender scenarios, or Bayesian methods to predict threat probabilities that evolve over time in response to observed conditions and monitored behavior provide more appropriate ways of representing the decisions of intelligent adversaries and should be explored.

Basis for Threat of Terrorism Risk

The data available to support assessments of threat can be grouped into three categories:

1. Expert opinions derived from intelligence analyses and formalized elicitation methodologies;
2. Physical, analytical, and engineering simulations; and
3. Historical data, including statistics on past terrorist events worldwide, social sciences research into terrorists' behavior, journalist accounts, and terrorists' own writings about motivation and intent.

Expert Opinions

Individual judgments based on an assessment of available data by intelligence or related experts, or formal expert elicitation involving structured questions to assess probabilities across multiple experts, are often the best that can be achieved when rapid response is needed to address security threats. The objective should be to provide those making these judgments with as much objective information and decision support as possible, using our best knowledge from studies of human performance for such tasks. Significant research has been conducted on the performance of expert elicitation (Cooke, 1991; Cooke and Goossens, 2000; Cooke et al., 2007; Coppersmith et al., 2006; European Commission, 2000; Garthwaite et al., 2005; Hora, 1992; Keeney and von Winterfeldt, 1991; MacDonald et al., 2008; Morgan and Henrion, 1990; Morgan and Keith, 1995; O'Hagan et al., 2006; Otway and von Winterfeldt, 1992; Zickfeld et al., 2007). Formal methods attempt to counter biases that commonly arise in both lay and expert assessments of probabilities (Cullen and Small, 2004; NRC, 1996).

Expert elicitation has been used in homeland security applications for threat assessment in the Risk Management Solutions (RMS) Probabilistic Terrorism Model (Willis, 2007; Willis et al., 2005), for vulnerability assessments (see discussion of Critical Infrastructure and Key Resources [CIKR] risk analysis in Chapter 2), for consequence analysis (e.g., Barker and Haimes, 2009), and in other applications.[4] However, there has in general been a lack of guidance as to when and how formal expert elicitation techniques should be used in DHS assessments. The Environmental Protection Agency (EPA) published a white paper on the uses of expert elicitation for its regulatory assessments, and DHS should determine the extent to which this or a similar effort would be beneficial in its risk assessment guidance (see *http://www.epa.gov/osa/spc/expertelicitation/*).

[4] The DHS CREATE center has helped DHS with expert elicitation.

Physical, Analytical, and Engineering Simulations

The most rigorous approaches to risk assessment use structured system models to evaluate vulnerability and consequence. These often take the form of event or fault trees (Fovino et al., 2009; Sherali et al. 2008; Shindo et al., 2000), and may include predictive models for structural integrity and response (Davidson et al., 2005; Remennikov, 2003); outdoor and indoor air pollution and exposure (Fennelly et al., 2004; Fitch et al., 2003; Settles, 2006; Wang and Chen, 2008); drinking water distribution systems and detection of contamination events (Lindley and Buchberger, 2002; NRC, 2007b; Ostfeld et al., 2008); infrastructure dependence and interoperability (Haimes et al., 2005, 2008; Robert et al., 2008); and other specific system models, depending on the asset and its modes of vulnerability and consequence. While models of this type are always undergoing improvement, their formulation and parameterization remains highly uncertain, and this uncertainty must be explicitly addressed. The NISAC work discussed in Chapter 2 falls into this category.

Historical Data

Statistical analysis of observed data is most applicable in cases where extensive historical data are available. Terrorism risk analysis is hampered by datasets that are too sparse and targeted events that are too situation specific. When limited data are available, Bayesian statistical methods provide a means for updating expert beliefs (which provide *prior* probabilities) with the evidence of observed data to obtain *posterior* probabilities that combine the information from both sources (Berry and Stangl, 1996; Iman and Hora, 1989; Greenland, 2001, 2006; Guzzetti et al., 2005; Wolfson et al., 1996).

Challenges Facing Vulnerability Analysis

Vulnerability analyses for terrorism risk analysis also tend to rely heavily on expert judgments. As such, the general comments above regarding methods for ensuring reliable elicitation apply. The quality of a vulnerability analysis depends in part on the thoroughness with which information is gathered and vetted and on the capabilities of those involved to identify vulnerabilities that might not be caught by a standard process. The committee was told that the process used by the Office of Infrastructure Protection (IP) is heavily oriented toward physical security, and that it will not capture all the relevant vulnerabilities for some assets and sectors. There is also a tendency toward false precision, which is discussed in detail in Chapter 4.

Challenges Facing Consequence Analysis

The fundamental challenge for analyzing the consequences of a terrorist event is how to measure the intangible and secondary effects. DHS's consequence analyses tend to limit themselves to deaths, physical damage, first-order economic effects, and in some cases, injuries and illness. Other effects, such as interdependencies, business interruptions, and social and psychological ramifications, are not always modeled, yet for terrorism events these could have more impact than those consequences that are currently included. This is discussed in Chapter 4. Even though DHS is not responsible for managing all these aspects of risk—for example, the Department of Health and Human Services has the primary responsibility for managing public health risks—it is appropriate and necessary to consider the full spectrum of consequences when performing risk analyses.

BOX 3-2
Synopsis of Challenges for Risk Analysis in DHS

- Availability and reliability of data
- Modeling the decision making and behaviors of intelligent adversaries
- Appropriately characterizing and communicating uncertainty in models, data inputs, and results
- Methodological issues around implementing risk as a function of threats, vulnerabilities, and consequences
- Modeling cascading risks across infrastructures and sectors
- Incorporating broader social consequences
- Dealing with different perceptions and behaviors about terrorism versus natural hazards
- Providing analyses of value to multiple, distributed decision makers
- Varying levels of access to necessary information for analysis and decision making
- Developing risk analysis communication strategies for various stakeholders

4
Evaluation of DHS Risk Analysis

In evaluating the quality of Department of Homeland Security's (DHS's) approach to risk analysis—element (a) of this study's Statement of Task—we must differentiate between DHS's overall conceptualization of the challenge and its many actual implementations. Within the former category, the department has set up processes that encourage disciplined discussions of threats, vulnerabilities, and consequences, and it has established the beginning of a risk-aware culture. For example, the interim Integrated Risk Management Framework (IRMF), including the risk lexicon and analytical guidelines (primers) being developed to flesh it out, represents a reasonable first step. The National Infrastructure Protection Plan (NIPP) has appropriately stipulated the following four "core criteria" for risk assessments: that they be documented, reproducible, defensible, and complete (DHS-IP, 2009, p. 34). Similarly, the Office of Risk Management and Analysis (RMA) has stated that DHS's integrated risk management should be flexible, interoperable, and transparent and based on sound analysis.

Some of the tools within DHS's risk analysis arsenal are adequate in principle, if applied well; thus, in response to element (b) of the Statement of Task, the committee concludes that DHS has some of the basic capabilities in risk analysis for some portions of its mission. The committee also concludes that *Risk = A Function of Threat, Vulnerability, and Consequences* (Risk = $f(T,V,C)$) is a philosophically suitable framework for breaking risk into its component elements. Such a conceptual approach to analyzing risks from natural and man-made hazards is not new, and the special case of Risk = $T \times V \times C$ has been in various stages of development and refinement for many years. However, the committee concludes that Risk = $T \times V \times C$ is not an adequate calculation tool for estimating risk in the terrorism domain, for which independence of threats, vulnerabilities, and consequences does not typically hold and feedbacks exist. In principle, it is possible to estimate conditional probability distributions for T, V, and C that capture the interdependencies and can still be multiplied to estimate risk, but the feedbacks—the way choices that affect one factor influence the others—cannot be represented so simply.

Based on the committee's review of the six methods and additional presentations made by DHS to the committee, there are numerous shortcomings in the implementation of the Risk = $f(T,V,C)$ framework. In its interactions the committee found that many of DHS's risk analysis models and processes are weak—for example, because of undue complexity that undercuts their transparency and,

hence, their usefulness to risk managers and their amenability to validation—and are not on a trajectory to improve. The core principles for risk assessment cited above have not been achieved in most cases, especially with regard to the goals that they be documented, reproducible, transparent, and defensible.

This chapter begins with the committee's evaluation of the quality of risk analysis in the six illustrative models and methods that it investigated in depth. Then it discusses some general approaches for improving those capabilities.

DETAILED EVALUATION OF THE SIX ILLUSTRATIVE RISK MODELS EXAMINED IN THIS STUDY

Natural Hazards Analysis

There is a solid foundation of data, models, and scholarship to underpin the Federal Emergency Management Agency's (FEMA's) risk analyses for earthquakes, flooding, and hurricanes which uses the Risk = $T \times V \times C$ model. This paradigm has been applied to natural hazards, especially flooding, more than a century. Perhaps the earliest use of the Risk = $T \times V \times C$ model—often referred to as "probabilistic risk assessment" in other fields—dates to its use in forecasting flood risks on the Thames in the nineteenth century. In present practice, FEMA's freely-available software application HAZUS™ provides a widely used analytical model for combining threat information on natural hazards (earthquakes, flooding, and hurricanes) with consequences to existing inventories of building stocks and infrastructures as collected in the federal census and other databases (Schneider and Schauer, 2006).

For natural hazards, the term "threat" is represented by the annual exceedance probability distribution of extreme events associated with specific physical processes, such as earthquakes, volcanoes, or floods. The assessment of such threats is often conducted by applying statistical modeling techniques to the record of events that have occurred at the site or at sites similar to that of interest. Typically a frequentist approach is employed, where the direct statistical experience of occurrences at the site is used to estimate event frequency. In many cases, evidence of extreme natural events that precede the period of systematic monitoring can be used to greatly extend the period of historical observation. Sometimes regional information from adjacent or remote sites can be used to help define the annual exceedance probability (AEP) of events throughout a region. For example, in estimating flood frequencies in a particular river the historical period of recorded flows may be only 50 to 100 years. Clearly, that record cannot provide the foundation for statistical estimates of 1,000-year events except with very large uncertainty, nor can it represent with certainty probabilities that might be affected by overarching systemic change, such as from climate changes. To supplement the instrumental record, the frequency of

paleoflows is inferred from regional geomorphologic evidence and is being increasingly used. These are often incorporated in the statistical record using Bayesian methods in which prior, nonstatistical information can be used to enhance the statistical estimates. Other prior information may arise from physical modeling, expert opinions, or similar non-historical data.

The vulnerability term in the Risk = $T \times V \times C$ model is the conditional probability of protective systems or infrastructure failing to contain a particular hazardous event. For example, the hurricane protection system (HPS) of New Orleans, consisting of levees, flood walls, gates, and pumping stations, was constructed to protect the city from storm surges caused by hurricanes of a chosen severity (the design storm). In the event of Hurricane Katrina, the HPS failed to protect the city. In some areas the storm surge overtopped the levee system (i.e., the surge was higher than that for which the system was designed), and in some areas the system collapsed at lower water levels than those for which the HPS was designed because the foundation soils were weaker than anticipated. The chance that the protective system fails under the loads imposed by the threat is the vulnerability.

For most natural hazard risk assessments such as that performed for New Orleans (Interagency Performance Task Force, 2009), the vulnerability assessment is based on engineering or other physics-based modeling. For some problems, such as storm surge protection, these vulnerability studies can be complicated and expensive, involving multiple experts, high-performance computer modeling, and detailed statistical analysis. For other problems, such as riverine flooding in the absence of structural protection, the vulnerability assessment requires little more than ascertaining whether flood waters rise to the level of a building.

Assessing consequences of extreme events of natural hazards has typically focused on loss of lives, injuries, and resulting economic losses. Such assessment provides valuable knowledge about a number of the principal effects of natural disasters and other events. The assessment of natural disaster risks is quite advanced on these dimensions of consequences. These consequences can be estimated based on an understanding of the physical phenomena, such as ground acceleration in an earthquake or the extent and depth of inundation associated with a flood. Statistical models based on the historical record of consequences have become commonly available for many hazards. Statistical models, however, especially for loss of life, usually suffer from limited historical data. For example, according to information from the U.S. Geological Survey (USGS; *http://ks.water.usgs.gov/pubs/fact-sheets/fs.024-00.html*), only about 20 riverine floods in the United States since 1900 have involved 10 or more deaths. This complicates the validation of models predicting the number of fatalities in a future flood. As a result, increasing effort is being invested in developing predictive models based on geospatial databases (e.g., census or real property data) and simulation or agent-based methods. These techniques are maturing and appear capable of representing at least the economic and loss-of-life consequences for natural disasters. The National Infrastructure Simulation and

Analysis Center (NISAC) is advancing the state of art of natural hazard consequence analysis by studying the resiliency and interrelated failure modes of critical infrastructure.

Still, the full range of consequences of natural hazard events includes effects that lie outside current evaluations, such as loss of potable water, housing, and other basic services; diverse effects on communities; impacts on social trust; psychological effects of disasters; distributional inequities; and differential social vulnerability.[1] In addition, social and behavioral issues enter into response systems (e.g., community preparedness and human behavior from warnings during emergencies). Indeed, the second national assessment of natural hazards (Mileti, 1999) listed as one of its major recommendations the need to "take a broader, more generous view of social forces and their role in hazards and disasters." As risk assessment of natural hazards moves forward over the longer term, incorporating social dimensions into risk assessment and risk management will have to be a major priority in building a more complete and robust base of knowledge to inform decisions.

While models are constantly being developed and improved, risk analysis associated with natural hazards is a mature activity in which analytical techniques are subject to adequate quality assurance and quality control, and verification and validation procedures are commonly used. Quality control practices are actions taken by modelers or contractors to eliminate mistakes and errors. Quality assurance is the process used by an agency or user to ensure that good quality control procedures have in fact been employed. Verification means that the mathematical representations or software applications used to model risk actually do the calculations and return the results that are intended. Validation means that the risk models produce results that can be replicated in the world. To achieve this last goal, studies are frequently conducted retrospectively to compare predictions with actual observed outcomes.

A second indicator that risk analyses for natural hazards are fairly reliable is that the limitations of the constituent models are well known and adequately documented. For example, in seismic risk assessment the standard current model is attributed to Cornell (1968). This model identifies discrete seismic source zones, assigns seismicity rates (events per time) and intensities (probability distributions of the size of the events) to each zone, simulates the occurrence of seismic events, and for each simulated event, mathematically attenuates peak ground accelerations to the site in question according to one of a number of attenuation models. Each component of Cornell's probabilistic seismic hazard model is based on either statistics or physics. The assumptions of each component are identified clearly, the parameters are based on historical data or well-documented expert elicitations using standard protocols, and the major limitations (e.g., assuming log-linearity of a relationship when data suggest some nonlinearity) have been identified and studied.

It is important to note, however, that there are aspects of natural hazard dis-

[1] See Heinz Center (2000) for examples of recent research.

asters that are less easily quantifiable. With regard to the "vulnerability" component, a well-established base of empirical research reveals that specific population segments are more likely to experience loss of life, threatened livelihoods, and mental distress in disasters. Major factors that influence this social vulnerability include lack of access to resources, limited access to political influence and representation, social capital including social networks and connections, certain beliefs and customs, frail health and physical limitations, the quality and age of building stock, and the type and density of infrastructure and lifelines (NRC, 2006). Natural disasters can produce a range of social and economic consequences. For example, major floods disrupt transportation networks and public health services, and they interfere with business activities creating indirect economic impacts. The eastern Canadian ice storm of 1998 and the resulting power blackout, while having moderate direct economic impact, led to catastrophic indirect economic and social impacts. Transportation, electricity, and water utilities were adversely affected or shut down for weeks (Mileti, 1999). An indirect impact seldom recognized in planning is that among small businesses shut down by floods, fires, earthquakes, tornadoes, or major storms, a large fraction never reopen.[2]

An important consideration in judging the reliability of risk analysis procedures and models is that the attendant uncertainties in their results be identifiable and quantifiable. For example, in flood risk assessments the analytical process may be divided into four steps, along the Risk = $T \times V \times C$ model (Table 4-1). The discharge (water volume per time) of the river is the threat. The frequency of various river discharges is estimated from historical instrumental records. This estimates the inherent randomness in natural river flows (i.e., the randomness of nature) and is called aleatory uncertainty. Because the historical record is limited to perhaps several decades, and is usually shorter than a century, there is statistical error in the estimates of aleatory frequencies. There is also uncertainty in the model itself (i.e., the uncertainty due to limited data), which is called epistemic uncertainty. Each of the terms in the *TVC* model has both aleatory and epistemic uncertainties. In making risk assessments, good practice is either to state the final aleatory frequency with confidence bounds representing the epistemic uncertainty (typical of the relative frequency approach) or to integrate aleatory and epistemic uncertainty together into a single probability distribution (typical of the Bayesian approach).

An important characteristic of mature risk assessment methods is that the (epistemic) uncertainty is identifiable and quantifiable. This is the case for most natural hazards risk assessments. To say, however, that the uncertainties are identifiable and quantifiable is not to say that they are necessarily small. A range of uncertainty, in terms of a factor ranging from 3 to 10 or even more, is not uncommon in mature risk assessments, not only of natural hazards but of

[2] A report from the Insurance Council of Australia, *Non-insurance and Under-insurance Survey 2002*, estimates that 70 percent of small businesses that are underinsured or uninsured do not survive a major disaster such as a storm or fire.

TABLE 4-1 Risk = T × V × C: TVC components of Natural Hazard Risk Methodologies for Flood Risk

Risk = *T* × *V* × *C*	Component of Analysis	Prediction	Frequency (Aleatory)	Uncertainty (Epistemic)	
				Routinely Addressed	Deeper Uncertainties
T	Flood frequency	River discharge (flux)	Annual exceedance probability	Statistical parameters of regression equation for stream flow	Nonstationarity introduced by watershed development and climate change
V	River hydraulics	Stage (height) of river for given discharge	Probability distribution for given discharge	Model parameters of stage-discharge relationship	Channel realignment during extreme floods
	Levee performance	Does levee withstand river stage?	Probability that levee withstands water load of given stage	Geotechnical uncertainties about soil's foundations	Future levee maintenance uncertain
C	Consequences	Direct economic loss to structures in the flood-plain	Probability distribution of property losses for flood of given extent	Statistical imprecision in depth-damage relations from historical data	Enhanced protection induces flood-plain development and increased damages

industrial hazards as well (e.g., Bedford and Cooke, 2001). These uncertainty bounds are not a result of the risk assessment itself: the uncertainties reside in our historical and physical understandings of the natural and social processes involved. They are present in deterministic design studies as well as in risk assessments, although in the former they are masked by factors of safety and other traditional means of risk reduction.

Conclusion: DHS's risk analysis models for natural hazards are near the state of the art. These models—which are applied mostly to earthquake, flood, and hurricane hazards—are based on extensive data, have been validated empirically, and appear well suited to near-term decision needs.

Recommendation: DHS's current natural hazard risk analysis models, while adequate for near-term decisions, should evolve to support longer-term risk management and policy decisions. Improvements should be made to take into account the consequences of social disruption caused by natural hazards; address long-term systemic uncertainties, such as those arising from effects of climate change; incorporate diverse perceptions of risk impacts; support decision making at local and regional levels; and address the effects of cascading impacts across infrastructure sectors.

Analyses of Critical Infrastructure and Key Resources (CIKR)

DHS has processes in place for eliciting threat and vulnerability information, for developing consequence assessments, and for integrating threat, vulnerability, and consequence information into risk information briefings to support decision making. Since CIKR analyses are divided into three component analyses (threat, vulnerability, and consequence) the committee reviewed and evaluated these component elements.

Threat Analyses

Based on the committee's discussions and briefings, DHS does strive to get the best and most relevant terrorism experts to assess threats. However, regular, consistent access to terrorism experts is very difficult. Due to competing priorities at other agencies, participation is in reality a function of who is available. This turnover of expertise can help prevent bias, but it does put a premium on ensuring that the training is adequate. Rotation of subject matter experts (SMEs) also puts a premium on documenting, testing, and validating assumptions, as discussed further below. Importantly, a disciplined and structured process for conducting the threat analysis is needed, but the current process as described to the committee was ad hoc and based on experts' availability.

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) has made efforts to inject imagination into risk assessments through processes such as red-team exercises. As a next step, there needs to be a systematic and defensible process by which ideas generated by red teams and through alternative analysis sessions are incorporated into the appropriate models and the development of new models.

Another concern is how the assumptions used by the SMEs are made visible and can be calibrated over time. The assumptions as to intent and capabilities that the SMEs make when assigning probabilities need to be documented. Attempts must be made to test the validity of these assumptions, as well as track and report on their reliability or correctness over time. Equally important is bringing to light and documenting dissenting views of experts, explaining how

they differ (in terms of gaps in information or in assumptions), and applying those results to inform future expert elicitation training and elicitation processes as well as modifying and updating the attack scenarios.

Many DHS investments, such as those made through the Homeland Security Grant Programs (HSGPs) in FEMA and CIKR protection programs, are meant to reduce vulnerabilities or increase resilience for the long term. DHS recognizes that the use of generic attack scenarios (threats) based on today's knowledge can leave risk analyses vulnerable to the unanticipated "never-before-seen" attack scenario (the black swan) or to being behind the curve in emerging terrorist tactics and techniques.[3] (For that reason, FEMA reduced the weighting of threat from 0.20 to 0.10 for some of the HSGPs so that the resulting risk prioritizations are less dependent on the assumptions about threat.) Attacks that differ from those DHS is currently defending against might have greater consequences or a higher chance of success. However, it is difficult to design a model to account for new tactics, techniques, or weapons. Asking experts to "judge" what they have not yet observed (or perhaps even conceived, until the question is posed) is fraught with more subjective assumptions and issues. Also, introducing too many speculative threats adds to the assumptions and increases the uncertainties in the models; lengthy lists of speculative attack scenarios could be generated, but the inherent uncertainty can be disruptive, rather than helpful, to planning and decision making. There is a large, unsolved question of how to make a model that can capture emerging or new threats, and how to develop the best investment decisions for threats that might not appear for years.

To provide the best possible analyses of terrorism threats, DHS has a goal to incorporate more state and local threat information into its risk assessments and has started numerous outreach programs. I&A, for example, conducts a weekly conference call and an assortment of conferences with state and local partners such as the regional fusion centers, at which threat information is shared or "fused." I&A plans to use the fusion centers as one of its primary means of disseminating information to the local level and collecting information from the local level. DHS has made increasing the number and its resources of the regional fusion centers a priority. There are currently 72 fusion centers around the country, and I&A plans to deploy additional intelligence analysts to these centers. Between 2004 and the present, DHS has provided more than $320 million to state and local governments to support the establishment and maturation of fusion centers. In 2007 testimony to the House Committee on Homeland Security Subcommittee on Intelligence, the HITRAC Director said that as part of this outreach plan, "we are regularly meeting with Homeland Security Advisors and their staffs to integrate State information and their analysis into the creation of

[3] The Black Swan Theory refers to high-impact, hard-to-predict, and rare events beyond the realm of normal expectations. Unlike the philosophical "black swan problem," the "Black Swan Theory" (capitalized) refers only to events of large magnitude and consequence and their dominant role in history. Black Swan events are considered extreme outliers (Taleb, 2007).

state critical infrastructure threat assessments. By doing this we hope to gain a more comprehensive appreciation for the threats in the states" (Smislova, 2007).

Despite these efforts, information sharing between the national and local levels and among state and local governments still faces many hurdles. The most significant challenges are security policies and clearances, common standards for reporting and data tagging, numbers and skill levels of analysts at the state and local levels, and resources to mature the information technology (IT) architecture. The committee cannot assess the impact of all these efforts to increase the information and dialogue between national and local levels with respect to DHS risk analysis, and specifically with regard to threat assessments and probabilities. The majority of information gathered by the fusion centers is on criminal activities, not foreign terrorism. In a 2007 report by the Congressional Research Service, a DHS official was quoted as saying that the local threat data still were not being incorporated into threat assessments at the federal level in any systematic or meaningful manner (Masse et al., 2007, p. 13). The committee assumes that the fusion centers and processes need to mature before any significant impact can be observed or measured.

It is important that insights gained during expert elicitation processes about threats, attack scenarios, and data gaps be translated into requests that influence intelligence collection. DHS's I&A Directorate and HITRAC program have processes that generate collection requirements. Due to security constraints the committee did not receive a full understanding of this process or its adequacy, but such a process should be reviewed by a group of fully cleared outside experts to offer recommendations.

Recommendation: The intelligence data gathering and vetting process used by I&A and HITRAC should be fully documented and reviewed by an external group of cleared experts from the broader intelligence community. Such a step would strengthen DHS's intelligence gathering and usage, improve the process over time, and contribute to linkages among the relevant intelligence organizations.

Threat analyses can also be improved through more exploration of attack scenarios that are not considered in the generic attack scenarios presented to SMEs. DHS has tackled this problem by creating processes designed for imagining the future and trying to emulate terrorist thinking about new tactics and techniques. An example is HITRAC's analytic red teaming, which contributes new ideas on terrorist tactics and techniques. DHS has even engaged in brainstorming sessions where terrorism experts, infrastructure specialists, technology experts, and others work to generate possibilities. These efforts to inject imagination into risk assessments are necessary.

Recommendation: DHS should develop a systematic and defensible process by which ideas generated through red teaming and alternative analysis sessions get incorporated into the appropriate models and the de-

velopment of new models. DHS needs to regularly assess what leaps could be taken by terrorist groups and be poised to move new scenarios into the models when their likelihood increases, whether because of a change inferred about a terrorist group's intent or capabilities, the discovery or creation of new vulnerabilities as new technologies are introduced, or an increase in the consequences of such an attack. These thresholds need to be established and documented, and a repeatable process must be set up.

The committee's interactions with I&A staff during a committee meeting and a site visit to the Office of Infrastructure Protection (IP) did not reveal any formal processes or decision criteria for updating scenarios or threat analyses. The real payoff in linking DHS risk assessment processes and intelligence community collection operations and analysis lies in developing a shared understanding for assessing and discussing risk.[4] I&A and HITRAC have created many opportunities for DHS analysts to interact with members from agencies in the intelligence community through conferences, daily dialogue among analysts, analytic review processes, and personnel rotations, and all of these efforts are to be applauded. However, there also need to be specific, consistent, repeatable exchanges, and other actions focused just on risk modeling. These interactions with experts from the broader intelligence community—including those responsible for collection operations—should be focused on building a common terminology and understanding of the goals, limitations, and data needs specific to DHS risk assessments.

To forge this link in cultures around the threat basis of risk, even risk-focused exchanges might not be enough. There needs to be some common training and even perhaps joint development of the next generation of national security-related risk models.

Vulnerability Analyses

DHS's work in support of critical infrastructure protection has surely instigated and enabled more widespread examination of vulnerabilities, and this a positive move for homeland security. IP's process for conducting vulnerability analyses appears quite thorough within the constraints of how it has defined "vulnerability," as evidenced, for example, in its establishment of coordinating groups (Government Coordinating Councils and Sector Coordinating Councils) for each CIKR sector, to effect collaboration across levels of government and between government and the private sector. These councils encourage owners and operators (85 percent of whom are in the private sector) to conduct risk assessments and help establish expectations for the scope of those assessments (e.g., what range of threats to consider and how to assess vulnerabilities beyond

[4] While DHS is a part of the intelligence community, this subsection is focused on building ties and common understanding between DHS and the complete intelligence community.

simply physical security).[5] Vulnerability assessment tools have been created for the various CIKR sectors. IP has worked to create some consistency among these, but it appears to be flexible in considering sector-recommended changes. To date, it seems that vulnerability is heavily weighted toward site-based physical security considerations.

IP has also established the Protective Security Advisors (PSA) program, which places vulnerability specialists in the field to help local communities carry out site-based vulnerability assessments. The PSAs collect data for HITRAC use while working with CIKR site owners or operators on a structured assessment of facility protections, during which PSAs also provide advice and recommendations on how to improve site security. The committee was told by IP that the average time spent on such an assessment is 40 hours, so a significant amount of data is collected for each site and a detailed risk assessment is developed jointly by a PSA and the site owner-operator. Sites identified by HITRAC as high risk are visited at least yearly by a PSA. HITRAC is currently working on a project called the Infrastructure Vulnerability Assessment (IVA) that will integrate this site-specific vulnerability information with vulnerability assessments from Terrorism Risk Assessment and Measurement (TRAM), Transportation Security Administration (TSA), MSRAM, and elsewhere to create a more integrated picture of vulnerabilities to guide HITRAC risk assessment and management efforts.

However, vulnerability is much more than physical security; it is a complete systems process consisting at least of exposure, coping capability, and longer-term accommodation or adaptation. Exposure used to be the only thing people looked at in a vulnerability analysis; now there is consensus that at least these three dimensions have to be considered. The committee did not hear these sorts of issues being raised within DHS, and DHS staff members do not seem to be drawing from recent books on this subject.[6]

IP is also working toward combining vulnerability information to create what are called "Regional Resiliency Assessment Projects (RRAPs)," in an attempt to measure improvements in security infrastructure by site, by industry sector, and by cluster. RRAPs are analyses of groups of CIKR assets and perhaps their surrounding areas (what is known as the buffer zone, which is eligible for certain FEMA grants). The RRAP process uses a weighted scoring method to estimate a "regional index vulnerability score" for a cluster of CIKR assets, so that their risks can be managed jointly.

Examples of such clusters are New York City bridges, facilities surrounding Exit 14 on the New Jersey Turnpike, the Chicago Financial District, Raleigh-Durham Research Triangle, and the Tennessee Valley Authority.

However, the complexity of the RRAP methodology seems incommensu-

---

[5] *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, GAO-07-706R (July 10, 2007), evaluated the capabilities of a sample of these councils and found mixed results.

[6] See for example Ayyub et al., 2003; Bier and Azaiez, 2009; Bier et al., 2008; Haimes, 2008, 2009; McGill et al., 2007; and Zhuang and Bier, 2007.

rate with the innate uncertainty of the raw data. To determine the degree to which risk is reduced by investments in "hardening" of facilities (reduction of vulnerabilities), the RRAP process begins by asking SMEs (including PSAs and sector experts) to identify the key factors for security, rank them, estimate their relative importance, and aggregate those measures into a Protective Measure Index (PMI). For example, for physical security, the SMEs estimate those factors for fences, gates, parking, access control, and so forth, to develop weighted PMIs, which are the product of PMIs and a weight for each security component. The weighted PMIs were shown to four significant figures in a presentation to the committee, and different values are estimated for physical security, security forces, and security management. Those three weighted PMIs are averaged to obtain an overall index for a piece of critical infrastructure. Within a given region, the overall indexes for each relevant facility are likewise averaged to obtain a Regional Vulnerability Index (to four significant figures). Then, if certain of those facilities improve their security or otherwise reduce their vulnerabilities, the regional vulnerability is deemed to have dropped, and the change in Regional Vulnerability Index is taken as a measure of the degree to which risk has been bought down. It was not clear to the committee how, or even if, threat and consequence were folded into the buying down of risk. Using four significant figures is not justified, quite misleading, and an example of false precision.

An example shared with the committee, using notional data for a downtown area of Chicago, computed a Regional Vulnerability Index of 52.48 before hardening steps and an index of 68.78 after. The claim was made that these hypothetical steps have then led to "a 31.06 percent decrease in vulnerability." It is not clear what this 31.06 percent reduction actually means. Has the expected yearly loss been reduced by 31 percent (say from $1 billion to $690 million)? Have the expected casualties been reduced from 1,000 to 690? Is this a reduction on some normalized scale in which case the actual expected loss reduction could be significantly more? It would be essential to answer these questions if risks across DHS elements were being compared. Furthermore, it is difficult to believe that any of these metrics are as accurate as the numbers imply. If their accuracy is ±20 percent, the first Regional Vulnerability Index could just as readily be 63 (120 percent of 52.48), and the second could just as easily be 55 (80 percent of 68.78), in which case the relative vulnerabilities would be reversed. In addition, as noted earlier, the emphasis on physical security might in some cases divert attention from other aspects of vulnerability that would be more valuable if addressed.

Consequence Analyses

The consequence analyses done in support of infrastructure protection, mostly by NISAC, is carried out with skill. Recent requests for modeling and analysis at NISAC covered topics such as an influenza outbreak, projecting the economic impacts of Hurricane Ike around Houston, an electric power disrup-

tion around Washington, D.C., and evaluation of infrastructure disruption if there were an earthquake along the New Madrid Fault zone. The committee was told by NISAC that it has developed some 70-80 models or analysis tools for modeling consequences of disruptive events. However, in a number of cases examined by the committee, it is not clear what problem is being addressed (i.e., what decision is to be supported by the analysis). A clear example of this is a new project to explore a wide range of ramifications of an earthquake along the New Madrid Fault. Neither NISAC nor IP leaders could explain why the work had been commissioned, other than to build new modeling capabilities. One would hope that a risk analysis had been performed somewhere in DHS that identified such an earthquake as one of the highest-priority concerns of DHS, but if that decision was made, it does not seem to be the result of a documented risk analysis. Other NISAC analyses in support of well-recognized DHS concerns—one that examined the economic consequences of a hurricane hitting the Houston area and another evaluating the evolution of a flu outbreak, with and without different intervention options—still seemed disconnected from any real decision-making process. In both cases, the committee also was concerned about missed opportunities for validation.

IP and HITRAC rely primarily on NISAC for consequence analyses. However, the committee observed that documentation, model verification and validation, model calibration and back-testing, sensitivity analyses, and technical peer reviews—which are necessary to ensure that reliable science underlies those models and analyses—vary widely across the different models and analyses. For instance, after projection of the economic consequences from Hurricane Ike, no comparison was made between the simulated projections and actual data. NISAC modelers noted that the consequences would surely be different because the actual storm track was not the same as the projected storm track used in the model. Such a retrospective analysis would seem to provide useful feedback to the modelers. As an alternative, the models could have been run retrospectively with the actual storm track to compare to actual damage. In another example, NISAC conducted an analysis of likely ramifications of a flu outbreak, but no one compared those multidimensional results with what is known from many seasonal outbreaks of flu.

More generally, the committee makes the following recommendation about consequence modeling for CIKR analysis,[7] to bring them up to the standards of the core criteria[8] previously cited from the 2009 NIPP (DHS-IP, 2009).

Recommendation: DHS should ensure that vulnerability and consequence analyses for infrastructure protection are documented, transparent, and repeatable. DHS needs to agree on the data inputs, understand the

[7] The only consequence modeling that the committee examined in detail is that performed by NISAC, primarily in support of IP. Clearly, all consequence analyses need to be documented, transparent, repeatable, and based on solid science.

[8] The four "core criteria" for risk assessments: that they be documented, reproducible, defensible, and complete (DHS, 2009b).

technical approaches used in models, and understand how the models are calibrated, tested, validated, and supported over the lifecycle of use.

The committee was also concerned that none of DHS's consequence analyses—including, but not limited to, the analyses done in support of infrastructure protection—address all of the major impacts that would come about from a terrorist attack. Consequences of terrorism can range from economic losses to fatalities, injuries, illnesses, infrastructure damage, psychological and emotional strain, disruption to our way of life, and symbolic damage (e.g., an attack on the Statue of Liberty, Washington Monument, or Golden Gate Bridge). DHS had initially included National Icons in its CIKR lists but seemed to eliminate them from CIKR analyses over time, since it was not clear what metrics should be used to assess that dimension of risk.

Recommendation: The committee recommends focusing specific research at one of the DHS University Centers of Excellence to develop risk models and metrics for terrorism threats against national icons.

The range of consequences considered is also affected by the mandate of the entity performing the risk analysis. It should be DHS's role to counter limitations that occur because private owners-operators, cities, tribes, and states have boundaries (geographic and functional) that delimit their sphere of responsibility. A fundamental step to clarifying this role is for DHS to be very clear about the decision(s) to be informed by each risk analysis it develops. This is discussed below in the section titled "Guidelines for Risk Assessment and Transparency in Their Use for Decisions." There are people at DHS who are aware of these current limitations, but the committee did not hear of efforts to remedy them.

For example, when the Port Authority of New York and New Jersey evaluates the potential consequences of a terrorist attack on one of its facilities, it does not try to model larger-scale consequences such as social disruption; its mandate is to minimize the physical consequences of an attack on facilities under its control. From the standpoint of its management, that might be a good risk analysis, but it is not adequate for evaluating the real risk of such an attack.

Integration of Threat, Vulnerability, and Consequence Analyses

DHS is currently using Risk = $f(T,V,C)$ to decompose the overall analysis problem into more manageable components (i.e., a threat analysis to identify scenarios, a vulnerability analysis given threat scenarios, and a consequence analysis given successful threats against identified vulnerabilities). However, the component analyses themselves can be quite complex, and there exist theoretical as well as practical problems in combining these individual components into an aggregate measure of risk. For example, the performance of modern

infrastructures relies on the complicated interaction of interdependent system components, so C is in general dependent in complex, nonlinear ways on the particular combination of individual components that are affected by an attack or disaster.

When it comes to the interaction of intelligent adversaries, the assumption that it is possible to characterize the values of T and V as independent probabilities, even when assessed by SMEs, is problematic. Rasmussen noted this issue when he cautioned, "One of the basic assumptions [in the original WASH-1400 study] is that failures are basically random in nature… in the case of deliberate human action, as in imagined diversion scenarios, such an assumption is surely not valid" (Rasmussen, 1976). As noted by Cox (2009), the values for V and C depend on the allocation of effort by both the attacker and the defender.

Additional problems arise for different functional forms of the Risk = *f(T,V,C)* equation. For example, some models rely on the succinct product, $R = T \times V \times C$, where SMEs assess the threat and vulnerability terms as probabilities and the consequence terms in units of economic replacement costs or fatalities (ASME, 2008; Willis, 2007). The appeal here is simplicity, and the probabilities are conventionally drawn as numeric values attached to colors (e.g., red, yellow, green) assigned to cells in risk matrices. Cox (2008) illustrates with a number of simple examples how such formulas can render nonsensical advice.

Although the committee reviewed a number of specific component analyses, often it was unable to determine how the component analyses would actually be combined in the Risk = *f(T,V,C)* paradigm. In many cases, these analyses were conducted using different assumptions and for different reasons, making it very difficult to recombine components back into a Risk = *f(T,V,C)* calculation.

As a first example, the committee reviewed the 2007 pandemic influenza report prepared by NISAC, Infrastructure Analysis and Strategy Division, and IP. Seven scenarios of disease, response, and mitigation were determined and approved by the DHS Office of Health Affairs. Using these seven threat scenarios as inputs, NISAC exercised various simulation models to characterize the vulnerability of the U.S. population given the specific scenario. Vulnerability, conditional on exposure to influenza as described by the specific threat scenario, is measured in terms of estimated attack rate (proportion of the population that becomes infected during a set period of time) and estimated mortality rate (proportion of the population that dies from influenza during the set period of time). The vulnerability analysis also considers a typical seasonal influenza outbreak scenario, giving the decision maker estimates of attack rate and mortality rate for seasonal flu. Given each threat scenario and the associated rate of attack and mortality estimates (vulnerability estimates), the NISAC modelers calculated reduction in labor in critical infrastructure sectors (i.e., absenteeism rate and duration [population consequences]). Given these estimated population consequences, the modeling team then considered how workforce absenteeism would influence various CIKR sectors such as energy, water, telecommunications, public health and health care, transportation, agriculture and food, and banking and

finance. In reading the NISAC report, it is clear that the separate threat, vulnerability, and consequence analyses are not actually intended to be combined into a single risk measure, sidestepping the challenge of computing a risk measure and instead passing on component analyses under the assumption that decision makers could use their individual judgment to develop an understanding about the risks from an influenza outbreak.

As a second example, the committee reviewed the Chemical Facility Anti-Terrorism Standards (CFATS), a regulatory program run by DHS to address security at high-risk chemical facilities. Facilities that are deemed "high risk" are a subset of those that have certain dangerous chemicals onsite in quantities over designated thresholds. As a first step in identifying high-risk facilities that will be subject to DHS regulation, more than 29,000 were identified that met these thresholds for dangerous chemicals onsite, and each filled out a first-level quick questionnaire. Data were collected from site owner-operators through a web-based IT decision support system. A consequence screening of this data identified some 6,400 of the 29,000 facilities as being risky enough to merit DHS regulation. Those 6,400 facilities were sorted into four preliminary tiers, based on the riskiness of the site. Roughly speaking, the threats under consideration are those associated with terrorists releasing, stealing, sabotaging, or contaminating chemicals that are toxic, flammable or explosive. Risk appears to be based almost exclusively on consequences, which reflect casualties only. The committee was unable to determine exactly what went into this definition of risk, and no documentation was provided beyond briefing slides. It was unclear how vulnerability and threat are used in determining the risk rating of various facilities. Economic losses do not yet appear to be included. For each of these sites, a Security Vulnerability Assessment (SVA) and a Site Security Plan (SSP) are being developed. The SSP must demonstrate how the site will meet DHS regulatory standards. The CFATS Program currently has 20 inspectors who support site assessment visits and sign off and validate SSPs, and the committee was told that plans exist to increase that number soon to about 150.

Incorporation of Network Interdependencies

DHS, through a variety of activities, has made considerable progress in identifying and collecting relevant site-specific data that can be used for analyzing vulnerabilities and consequences within and across the 18 critical infrastructure sectors and in interdependent networks of operations. Such activities include the HITRAC Level 1/Level 2 program for differentiating high-risk targets, 18 Individual Sector Risk Profiles, development of a National Critical Foreign Dependencies list, deployment of PSAs to support Site Assistance Visits (SAVs), and the Enhanced Critical Infrastructure Protection Initiative (ECIP) that is under development.

One challenge that makes CIKR vulnerability and consequence analyses difficult is that multiple levels of analysis are required: federal, state, local,

tribal, regional, and site specific, for example. Further, while risk analysis to support protection and prevention investments are often implemented at the site-specific or local level,[9] the cost-benefit trade-offs to understand risk reduction effects must be assessed at multiple levels and in the broader context of maintaining and enhancing the functionality of critical interdependent infrastructure networks or clusters of operations. DHS has begun exploring how to aggregate site-based vulnerability analyses into analyses of infrastructure clusters or networks with Regional Resiliency Assessment Projects, as noted above. However, the current site-based and regional cluster vulnerability index scoring methods being used are very narrow in scope, focusing only on physical security criteria such as fences, gates, access control, and lighting.

A second challenge in analyzing CIKR is the decision time frame. Short-term vulnerability models can take intelligence about enemy intent as an input, and thus have some confidence (lower uncertainty) about the type of threat to defend against. Longer-term resiliency models (similar to those used in Department of Defense strategic planning) plan around capabilities needed to respond to and recover from a variety of possible disruption events, whether terrorist attacks, natural hazards, or industrial accidents. DHS recognizes the need for analysis and planning for both short-term protective measures and longer-term risk-based investments in prevention, protection, response, and resiliency. Site Assistance Visits conducted by DHS in partnership with other federal, state, and local entities and in collaboration with owners-operators of critical infrastructures, are reasonably well suited to identify vulnerabilities related to specific threats (as identified by the intelligence community), to provide security recommendations at critical sites, and to rapidly address and defend against such threats. For the longer-term infrastructure investment decisions, RRAPs have begun focusing on analyzing vulnerabilities in critical infrastructure clusters. While this methodology is a first step in performance-based facilities protection, the RRAP approach does not fully capture the disruption impact in interdependent networks of critical infrastructure, does not account for vulnerability criteria other than physical security at individual locations, and is not easily extendable to account for socioeconomic vulnerabilities in local workforce and community.

Eighty-five percent or more of the critical infrastructure is owned and operated by private entities, and DHS has established processes to enable it to work collaboratively with those entities. Infrastructure operators have much experience and financial incentive in dealing with and effectively recovering from all types of disruptions, such as accidents, system failures, machine breakdowns, and weather events. Yet by moving beyond the focus on protective security to a resilience modeling paradigm, DHS might find that the private sector owners-operators are even more amenable to collaboration on improving infrastructure, particularly because resilience models promote using common metrics of inter-

[9] See, for example, some of the state-of-the-art technical literature on site-based risk analysis and infrastructure protection, such as Ayyub et al., 2003; Bier et al., 2008; Bier and Azaiez, 2009; Haimes, 2008, 2009; McGill et al., 2007; and Zhuang and Bier, 2007.

est to both DHS and the private sector, namely the ability of a site to operate as intended and at lowest cost to provide critical products or services. Boards of directors of private sector companies tend to think about resilience in terms such as additional capacity, redundant physical operations, and suppliers. Security and resilience have a cost, and their impact on revenue generation is less clear because it is difficult to show the benefits of loss avoidance and the value of continuity plans and built-in system resiliency. Decades of work to develop lean, just-in-time manufacturing and service operations have led to systems that may also be brittle and easy to disrupt. Heal and Kunreuther (2007) and Kunreuther (2002) show the disincentives of individual firms to invest in security, unless all owners-operators in a sector agree to it simultaneously. This line of research provides insight for DHS to consider in developing federal policy or industry sector voluntary action to achieve sector-wide security goals. Recent work by Golany et al. (2009) has shown that optimal resource allocation policies can differ depending on whether a decision maker is interested in dealing with chance events (probabilistic risk) or events caused by willful adversaries.

Conclusion: These network disruption and systems resilience models (which supplant and move away from current limitations of *TVC* analyses for CIKR) are ideal for longer-term investment decisions and capabilities planning to enhance infrastructure systems' resiliency, beyond just site-based protection. Such models have been used in other private sector and military applications to assist decision-makers in improving continuity of operations.

Recommendation: DHS should continue to enhance CIKR data collection efforts and processes and should rapidly begin developing and using emerging state-of-the art network and systems disruption resiliency models to understand and characterize vulnerability and consequences of infrastructure disruptions.

Such network disruption and systems resiliency models have value for a variety of reasons. These models can be used to

1. Assess a single event at a single site, multiple simultaneous events at single or multiple sites, or cascading events at single or multiple sites;
2. Understand event impacts of terrorism attacks, industrial accidents, and natural hazards using a single common model (integrated all-hazards approach where threat is any disruption event that impacts system ability to function as intended);
3. Assess impacts of worst case when none of the response and mitigation options work, best case assuming all the response and mitigation options work, and any of the middle- ground response and mitigation scenarios in between;
4. Conduct threat, vulnerability, and consequence analyses in an integrated and straightforward manner;

5. Support multiscale modeling and analysis results "roll-up" (from site-based to local cluster to state-level, regional, and national impacts);

6. Analyze cost-benefit trade-offs for various protection and prevention investments, since investments are made typically at a single site but must be assessed at multiple levels to understand system benefits;

7. Allocate scarce resources optimally within and across 18 interdependent CIKR sectors to maximize system resilience (ability of a network of operations or interdependent cluster of sites to function as intended)—in particular, such return-on-investment analyses are intended to help identify and justify budget levels to enhance security and resilience;

8. Evaluate interdiction and mitigation "what-if" options in advance of events, optimize resource allocation, and improve response and recovery;

9. Measure and track investments and improvement in overall system resiliency over time;

10. Provide a common scalable framework for modeling interdependencies within and across CIKR sectors;

11. Easily and visually demonstrate disruption events and ripple effects for table-top exercises; and

12. Incorporate multiple measures and performance criteria so that multiple stakeholders and multiple decision makers can understand decisions and compare risks in a single common integrated network-system framework.

This modeling approach has a long history in the operations research academic and practitioner communities, is mathematically well accepted, and technically defensible, and permits peer review and documentation of models, whether modelers use optimization, simulation, game-theoretic, defender-attacker-defender, or other approaches to analyze decisions in the CIKR networks.[10] More broadly, this approach has been applied successfully across industry sectors for supply chain risk analysis,[11] military or defense assets planning,[12] airline irregular operations recovery (e.g., recovery of flight schedules interrupted due to bad weather, shutdown of a major airport hub),[13] and managing enterprise production capacity.[14] This type of approach has also been used successfully in conjunction with more traditional site-based facilities management and security or fire protection operations[15] and is recommended by the American Society of Civil Engineers' Critical Infrastructure Guidance Task Committee in its recently released *Guiding Principles for the Nation's Critical Infrastructure* (ASCE, 2009).

For example, over the past 10 years, the Department of Operations Research at the Naval Postgraduate School has offered an introductory master's level

[10] See Ahuja et al., 1993; Bazaraa and Sherali, 2004; and Golden, 1978.
[11] See Chapman et al., 2002; Elkins et al., 2004.
[12] See Cormican et al., 1998; Smith et al., 2007.
[13] See Barnhart, 2009; Yu and Qi, 2004.
[14] See Bakir and Savachkin, 2010; Savachkin et al., 2008.
[15] Elkins et al., 2007.

course to focus attention on network disruption and resilience analysis. In this course, graduate students identify critical infrastructure networks of various types from their technical areas of expertise (primarily associated with their military duty assignments) and use network analysis tools, publically available open source data, and rapid prototyping in Microsoft Excel, Microsoft Access, and Visual Basic for Applications to develop decision support tools. Students have conducted more than 100 studies of infrastructure networks spanning electric power transmission, water supplies, fuel logistics, key road and bridge systems, railways, mass transit, and Internet service providers. A few of these case studies and the bilevel or trilevel optimization approach used (i.e., defender-attacker or defender-attacker-defender sequential decision-making models) are described in recent journal articles, and they demonstrate both the technical rigor (including peer-review quality of model documentation) and the real-world applicability of this method (Alderson, 2008; Alderson et al., 2009; Brown et al., 2006). This sort of approach would seem to be of great value to DHS, and the committee was pleased to see some initial efforts by DHS-IP to tap into this knowledge base.

Recommendation: DHS should exploit the long experience of the military operations research community to advance DHS capabilities and expertise in network disruptions modeling and resiliency analysis.

Risk-Based Grant Allocations

In 2008, FEMA awarded more than 6,000 homeland security grants totaling over $7 billion. More than 15 grant programs administered by FEMA that are designed to enhance the nation's capability to reduce risks from manmade and natural disasters, all of which are authorized and appropriated through the normal political process. Some have histories dating to the establishment of FEMA in the mid-1970s.

Five of these programs, covering more than half of FEMA's grant money—the State Homeland Security Program, the Urban Areas Security Initiative, the Port Security Grant Program, the Transit Security Grant Program, and the Interoperable Emergency Communications Grant Program—incorporate some form of risk analysis in support of planning and decision making. Two others inherit some risk-based inputs produced by other DHS entities—the Buffer Zone Protection Program, which allocates grants to jurisdictions near critical infrastructure if they are exposed to risk above a certain level as ascertained by the Office of Infrastructure Protection; and the Operation Stonegarden Grant Program, which provides funding to localities near sections of the U.S. border that have been identified as high risk by Customs and Border Patrol. All other FEMA grants are distributed according to formula.

FEMA has limited latitude with respect to tailoring even the risk-based grant programs, and the grants organization does not claim to be expert in risk.

Congress has defined which entities are eligible to apply for grants, and for the program of grants to states it has determined that every state will be awarded at least a minimum amount of funding. Congress stipulated that risk is to be evaluated as a function of T, V, and C, and it also stipulated that consequences should reflect economic effects, and population, and should take special account of the presence of military facilities and CIKR.

However, FEMA *is* free to create the formula by which it estimates consequences and how it incorporates *T*, *V*, and *C* into an overall estimate of risk. For example, it has set vulnerability equal to 1.0, effectively removing that factor from the risk equation. That move was driven in part by the difficulty of performing vulnerability analyses for all the entities that might apply to the grants programs. FEMA does not have the staff to do that, and the grant allocation time line set by Congress is too aggressive to allow applicant-by-applicant vulnerability analyses. Also, although Congress has specified which threats are to be included in the analyses, DHS has latitude to define which kinds of actors it will consider. In the past, it defined threat for grant making as consisting solely of the threat from foreign terrorist groups or from groups that are inspired by foreign terrorists. That definition means that the threat from narcoterrorism, domestic terrorism, or other such sources was not considered.

For most grant allocation programs, FEMA weights the threat as contributing 20 percent to overall risk and consequence as contributing 80 percent. For some programs that serve multihazard preparedness, those weights have been adjusted to 10 percent and 90 percent in order to lessen the effect that the threat of terrorism has on the prioritizations. Because threat has a small effect on FEMA's risk analysis and population is the dominant contributor to the consequence term, the risk analysis formula used for grant making can be construed as one that, to a first approximation, merely uses population as a surrogate for risk. FEMA staff told a committee delegation on a site visit that this coarse approximation is relatively acceptable to the entities supported by the grants programs.

It appears that the choice of weightings in these risk assessments, and the parameters in the consequence formulas, are chosen in an ad hoc fashion and have not been peer reviewed by technical experts external to DHS. Such a review should be carried out at a more detailed level, and by people with specific, targeted expertise, than was feasible for the committee.

Recommendation: FEMA should undertake an external peer review by technical experts outside DHS of its risk-informed formulas for grant allocation to identify any logical flaws with the formulas, evaluate the ramifications of the choices of weightings and parameters in the consequence formulas, and improve the transparency of these crude risk models.

Recommendation: FEMA should be explicit about using population density as the primary determinant for grant allocations.

Since a large majority of the grants programs are terrorism related, grant applicants write targeted grant applications to qualify for terrorism-related fund-

ing. At the same time, grantees clearly recognize the potential multiuse benefits of investment in community infrastructure and preparedness (e.g., hospital infrastructure investments to respond to bioterrorism are also useful in dealing with a large food poisoning outbreak). In response to the grassroots understanding in the public planning, public health, and emergency response professional communities of the potential compounding benefits of investments in community preparedness, response, and recovery, FEMA is exploring a Cost-to-Capability (C2C) Initiative as explained in Chapter 2. C2C is a "model" to "develop, test, and implement a method for strategically managing a portfolio of grant programs at the local, state, and federal levels." It is intended to "create a culture of measurement, connect grant dollars to homeland security priorities, and demonstrate contributions of preparedness grants to the national preparedness mission."[16]

The C2C model replaces "vulnerability" with "capability," in a sense replacing a measure of gaps with a measure of the ability of a system or community to withstand an attack or disaster or to respond to it. These measures of local hardness can more readily be aggregated to produce regional and national measures of security—a macro measure of national "hardness" against homeland security hazards—whereas vulnerabilities are inherently localized: there is no definition of national vulnerability. A focus on hardening of systems will emphasize those steps that stakeholders wish to address proactively, whereas a focus on vulnerabilities can be a distraction because some vulnerabilities are acceptable and need not be addressed. Conceptually, it makes sense to think of building up capabilities in order to add to our collective homeland security.

While the C2C initiative is clearly in a conceptual stage, it appears to be a reasonable platform by which the homeland security community can begin charting a better path toward preparedness. A contractor is creating simple, Java-based software, which is now ready for its first pilot test. This software is intended to allow DHS grantees to perform self-assessments of the value of their preparedness projects, create multiple investment portfolios and rank them, and track portfolio performance. The plans are to distribute this software to the field so that grantees themselves can use it. It has not yet been vetted by outsiders, although the upcoming pilot test will begin that process.

Recommendation: FEMA should obtain peer review by experts external to DHS of the C2C concepts and plans, with the goal of clarifying ideas about measures, return on investment, and the overall strategy.

[16] Ross Ashley presentation July 8, 2009, Washington, D.C. subgroup meeting with FEMA to discuss Homeland Security Grants Program and Cost-to-Capability Initiative.

TRAM

The general framework for TRAM is fairly standard Risk = $f(T,V,C)$ risk analysis. The tool provides value by enforcing a rigorous, disciplined examination of threats, vulnerabilities, and consequences. Its outputs present a comparative depiction of risk against critical assets that is useful to inform decision makers.

However, the TRAM methodology appears to be unduly complex, given the necessarily speculative nature of the *TVC* analysis. For example, as part of the threat analysis, SMEs are guided to assess how attractive various assets are to potential terrorists. They do this by assigning a number on a scale of 1 to 5 for factors that are assumed to be important to terrorists (e.g., potential casualties associated with a successful attack, potential economic impact of a successful attack, symbolic importance). The SMEs are also asked to decide the scale of importance to terrorists of each of those factors, and this provides a weighting. Each value assessment is multiplied by the weight of that factor, and the products are summed to develop numbers that represent the "target value" of each asset. A similar process is followed to develop numbers that represent the deterrence associated with each asset. Deterrence factors are aspects such as the apparent security and visibility of each asset, and SME are also asked to weight those factors. The weighted sum for deterrence is multiplied by the target value to arrive at a "target attractiveness" number for each asset. It is unlikely that SMEs can reliably estimate so many factors and weightings from their small body of experience, so this complexity is unsupportable. Also, rather than attaching some measure of uncertainty to this concatenation of estimates, the TRAM experts who presented to the committee at its first meeting gave notional target attractiveness numbers to three significant figures, which implies much more certainty and precision than can be justified.

Overall, TRAM produces a threat rating for various attack scenarios that is calculated as the product of an SME rating of the attack likelihood and an SME rating of the scenario likelihood. The presentation of notional results at the committee's first meeting showed scenario likelihoods for a range of assets to three significant figures, which is unrealistic, and overall threat ratings for each of those assets (the product of attack likelihood and scenario likelihoods) to four significant figures.

Another indication of unsupportable complexity is the way that TRAM develops what is called Criticality Assessment. A set of Critical Asset Factors (CAFs) is defined, which represents different ways in which loss or damage of an asset will affect overall operations. CAFS include dimensions such as the potential for casualties, potential for business continuity loss, potential national strategic importance, potential economic impact, potential loss of emergency response function, and so on.[17] For each asset considered in the risk analysis, the effect of a given attack on each CAF for that asset is subjectively assessed

[17] From *TRAM Methodology Description,* dated May 13, 2009.

on a scale of 0 to 10, and other numbers between 1 and 5 are assigned to each CAF to reflect that factor's importance to the jurisdiction. Ultimately, the severity estimates are multiplied by the importance estimates (weights) and summed. This process introduces unnecessary complexity, a loss of transparency, and the possibility of misleading assessments of criticality. In some categories an arbitrary upper cap must be imposed.

TRAM vulnerability computation uses the product of three factors, each of which would seem to be a very uncertain estimate. The factors are called Access Control (likelihood that access will be denied), Detection Capabilities (likelihood that the attack would be detected), and Interdiction Capabilities (likelihood that the attack, if detected, will be interdicted). These estimates are different for each type of asset, each type of attack, and each class of security countermeasure. Each of these factors ranges from 0.0 to 1.0, again implying a sense of speculation. The difference between, say, a 0.5 and a 0.6 must be fairly arbitrary, so it is likely that the uncertainty is greater than ±10 percent for each of these SME-generated numbers.

Later in the process, TRAM estimates Response Capability Factors for capabilities such as law enforcement, fire service, and emergency medical services. The assessment for each is the product of rankings (from 0.0 to 1.0) of staffing, training, equipment, planning, exercise, and organizational abilities, all equally weighted.

Users of TRAM should be wary of assuming too much about its reliability. For example, the calculations leading to Threat Ratings and Target Attractiveness rely on SME estimates of numerous factors that may or may not be independent, none of which can be known with much certainty. Then weightings and (in the case of Target Attractiveness) a guess at Attack Elasticity are factored into the calculations. Similarly complex calculations are included in the analyses of vulnerabilities and in an assessment of local emergency response capabilities, as noted in Chapter 2.

This complexity also makes it very difficult to evaluate the model. On a site visit to the Port Authority of New York and New Jersey, a committee delegation asked the TRAM contractor team whether the tool had been validated. The response was that the toolkit had undergone "face validation," meaning that SMEs have not seen it produce results that were counterintuitive or, if it did, the model was adjusted to preclude that sort of outcome. This sort of feedback is useful but incomplete. Because the model has not been peer reviewed by technical experts external to DHS or the contractor, or truly validated, it is impossible to know the extent of the complexity problem or the effectiveness of TRAM at addressing uncertainty.

Nevertheless, as mentioned at the beginning of this section, TRAM's structured approach and capability to assist decision makers by providing "informed" relative risk information should be recognized. A tool such as TRAM enforces a disciplined look at risk and provides the organization that uses it with the credibility of applying a recognized tool rather than relying on the unstructured "educated or experienced guesses" of agency personnel or the "gut feelings" of

SMEs. The outputs produced by TRAM appear quite useful as a means of conceptualizing the risk space and the relative rankings of various risks. The tool is apparently also quite helpful in displaying how various risk mitigation options affect those relative rankings, allowing some degree of benefit-cost analysis. However, because of the uncertainties associated with all of these outputs and the fact that the uncertainties are not well characterized, TRAM should be used cautiously. In its current status, TRAM's outputs lack transparency for users and present a misleading degree of mathematical precision.

Finally, it is claimed that the TRAM software can estimate the risk buydown from enhancing certain security systems. Revised scatter graphs are produced periodically that show how the risk to critical assets is redistributed following the implementation of various countermeasures or mitigation options, and in this way a benefit-cost analysis is achieved. However, when the tool is used for benefit-cost analysis, it produces only estimates of how the risk rankings change under various risk mitigation options, and these could be misleading. Contractor experts said they can estimate the uncertainty in these risk analyses, although the output becomes complicated, and that information is normally interpreted by contractor staff and not presented to the end users.

The Port Authority of New York and New Jersey (PANYNJ) is the first client for TRAM and has been assisting DHS and its contractors in the toolkit's development from its inception. The PANYNJ users of TRAM have not questioned whether the model is validated, and they do not seem to be bothered by its tendency toward overquantification. They seem pleased to have a disciplined process that helps their staff identify the full spectrum of risks facing the Port Authority, and leaders of the agency point out the liability advantages to following a recognized system of risk analysis.

TRAM and PANYNJ staff told the committee how DHS assisted in a particular project, to mitigate the risk of an explosive attack in a Port Authority asset. DHS assistance began with a computational simulation of a bomb blast, which showed that the damage could be more severe than PANYNJ engineers had judged based on their intuition. Given that vulnerability analysis, the TRAM team developed a range of mitigation steps—various combinations of reinforcement and additions to physical security—and estimated the risk buydown for each combination. Based on this analysis, Port Authority leadership was able to choose a mitigation strategy that fit within its risk tolerance and budget constraints. This was considered a successful application of TRAM.

Recommendation: DHS should seek expert, external peer review of the TRAM model in order to evaluate its reliability and recommend steps for strengthening it.

Biological Threat Risk Assessment Model

DHS's Biological Threat Risk Assessment (BTRA) model, which has been

used to produce biennial assessments of bioterrorism risks since 2006, was thoroughly reviewed by a 2008 NRC report. The primary recommendation of that report reads as follows (NRC, 2008, p. 5):

> The BTRA should not be used as a basis for decision making until the deficiencies noted in this report have been addressed and corrected. DHS should engage an independent, senior technical advisory panel to oversee this task. In its current form, the BTRA should not be used to assess the risk of biological, chemical, or radioactive threats (NRC, 2008, p.5).

The complexity of this model precludes transparency, and the present committee does not know how it could be validated. The lack of transparency potentially obscures large degrees of disagreement about and even ignorance of anticipated events. Even sensitivity analysis is difficult with such a complex model. Finally, the model's complexity means it can only be run by its developers at Battelle Memorial Institute, not by those responsible for bioterrorism risk management.

While DHS reports that it is responding to most of the recommendations in the 2008 NRC report, the response is incremental, and a much deeper change is necessary. The proposed responses will do little to reduce the great complexity of the BTRA model. That complexity requires many more SME estimates than can be justified by the small pool of relevant experts and their base of existing knowledge. The proposed response does not move away from the modeling of intelligent adversaries with estimated probabilities. Whether meant as a static assessment of risks or a tool for evaluating risk management options, these shortcomings undermine the method's reliability. Finally, the proposed response does not simplify the model and its instantiation in software in a way that would enable it to be of greater use to decision makers and risk managers (e.g., by allowing near-real-time exploration of what-if scenarios by stakeholders). Therefore, the committee has serious doubts about the usefulness and reliability of BTRA.

The committee's concerns about BTRA are echoed by the Department of Health and Human Services (DHHS), which declined to rely on the results of the 2006 or 2008 BTRA assessments, a Chemical Terrorism Risk Assessment (CTRA), or the 2008 integrated Chemical, Biological, Radiological, and Nuclear (CBRN) assessment that builds on BTRA and CTRA.[18] DHHS is responsible for the nation's preparedness to withstand and respond to a bioterror attack, and in order to learn more about how DHS coordinates with another federal agency in managing a homeland security risk, a delegation of committee members made a site visit to DHHS's Biomedical Advanced Research and Development Authority (BARDA), which is within the office of the Assistant Secretary for Pre-

[18] Staff from Biomedical Advanced Research and Development Authority (BARDA), Department of Health and Human Services, at the committee members' site visit to DHHS. May 6, 2009, Washington, D.C.

paredness and Response. According to BARDA's web site, it "provides an integrated, systematic approach to the development and purchase of the necessary vaccines, drugs, therapies, and diagnostic tools for public health medical emergencies. BARDA manages Project BioShield, which includes the procurement and advanced development of medical countermeasures for chemical, biological, radiological, and nuclear agents, as well as the advanced development and procurement of medical countermeasures for pandemic influenza and other emerging infectious diseases that fall outside the auspices of Project BioShield." BARDA provides subject matter input to DHS risk analyses and relies on DHS for threat analyses and risk assessments.

One fundamental reason that BARDA declined to rely on these DHS products is that it received only a document, without software or the primary data inputs, and thus could not conduct its own "what-if" analyses that could guide risk mitigation decision making. For example, DHHS would like to group those outcomes that require respiratory care, because then certain steps could provide preparedness against a range of agents. Neither BTRA nor CTRA allows a risk manager to adjust the output. More generally, BARDA staff expressed "frustration" because DHS provides such a limited set of information in comparison to the complex strategic decisions that DHHS must make. Staff gave the following examples:

- The amount of agent included in an aerosol release was not stated in the CTRA report. This lack of transparency about basic assumptions undermines the credibility of the information coming out of the models that bear on consequence management.
- BARDA's SMEs believe that DHS was asking the wrong questions for an upcoming CTRA, but DHS was not willing to change the questions.
- The consequence modeling in CTRA and BTRA is getting increasingly complicated. When DHHS pointed this out, it was told that simplifications are being slated for upgrades several years in the future.

One of the BARDA staff members said that if BARDA had DHS's database and intermediate results, DHHS would be able to make "much better decisions" than it can seeing just the end results of an analysis. Under those preferred conditions, BARDA could vary the inputs (i.e., conduct a sensitivity analysis) to make better risk management decisions. For example, it could see where investments would make the most difference—that is, which countermeasures provide the best return on investment. More generally, BARDA staff would like to see a process with more interaction at the strategic level, allowing DHS and DHHS staff to jointly identify risks in a more qualitative manner. This should include a better definition of the threat space, with DHS defining scenarios and representing the threats for which DHHS and other stakeholders must prepare for. From BARDA's perspective, the risk modeling is less important than getting key people together and red-teaming a particular threat.

BARDA clearly has a compelling need for reliable assessments of bioterror-

ism risk, and it is a primary customer for the BTRA. At the committee's site visit to BARDA, a DHS representative noted that Food and Drug Administration, the Department of Defense, and the White House Homeland Security Council are also customers of BTRA and that they are satisfied with the product.[19] However, the committee does not believe that that is a reason to disregard the valid concerns of DHHS.

Integrated Risk Management Framework

The committee can develop only a preliminary impression of DHS's adoption of the Integrated Risk Management Framework because, as a developing process rather than a model, it is not yet in its final state. That is normal: instantiations of Enterprise Risk Management (ERM) in the private sector may take several years of work, and the results might be difficult to judge until even later. ERM is still an evolving field of management science. Companies from regulated sectors (finance, insurance, utilities) are the leaders in ERM sophistication, but those in nonregulated sectors (e.g., General Motors, Reynolds Corp., Delta Airlines, Home Depot, Wal-Mart, Bristol-Myers Squibb) are also practicing elements of ERM.[20]

Other federal agencies have also begun exploring the applicability of ERM to their own internal management challenges.[21] It is an appealing construct because of its potential for breaking down the stovepipes that afflict many agencies. However, absent the profit-making motive of private industry (which gives companies a motivation for judiciously taking on some known risks), ERM does not map directly onto the management of a public entity. Government agencies recognize that they cannot simply adopt best practices in risk management from industry. In addition to the less-obvious "upside" of risk, government agencies might have more heterogeneous missions than a typical private sector corporation, and they might have responsibility to plan for rare events for which few data exist. In addition, societal expectations are vastly different for a government agency compared to a private firm, and many more stakeholder perspectives must be taken into account by government agencies when managing their risks.

Successful implementations of ERM in the private sector employee processes reveal risks and emerging challenges early and then manage them proactively. These processes are shared across units where possible, both to minimize the resources required and to enable comparison of risks and sharing of mitigation steps. Such ERM programs need not be large and their resource require-

[19] Statement from Steven Bennett, DHS-RMA at site visit to DHHS, May 6, 2009, Washington, D.C.
[20] For additional background, see, for example, United Kingdom Treasury, 2004; Office of Government Commerce, United Kingdom Cabinet Office, 2002.
[21] For example, a Government Accountability Office summit on ERM was held on October 21, 2009.

ments can be minimal because they leverage existing activities. However, it is often the case that the group implementing ERM must have clear "marching orders" from top management. Many corporations and businesses have identified a senior executive (i.e., chief financial officer, chief executive officer, or chief risk officer) and provided that person with explicit responsibility for overseeing the management of all risks across the enterprise.

At present, DHS's ERM efforts within the Office of Risk Management and Analysis appear to be on the right track.[22] RMA has established a Risk Steering Committee (RSC) for governance, it has inventoried current practices in risk analysis and risk management, it has begun working on coordination and communication, and it is developing longer-term plans. RMA is a modest-size office, and it "owns" very few of the risks within DHS's purview. In terms of identifying and managing risks that cut across DHS directorates, formation and management of the RSC is a key enabler. In practice so far, most committee meetings seem to involve a Tier 3 RSC that consists of lower-level staff who have been delegated responsibilities for their components. Agendas for two recent meetings of the Tier 3 RSC suggest that those two-hour meetings were focused on updates and information sharing.

A NUMBER OF ASPECTS OF DHS RISK ANALYSIS NEED ATTENTION

Based on its examination of these six illustrative risk analysis models and processes, the committee came to the following primary conclusion, which addresses element (a) of the Statement of Task:

Conclusion: DHS has established a conceptual framework for risk analysis (risk is a function of threat (*T*), vulnerability (*V*), and consequence (*C*), or $R = f(T,V,C)$) that, generally speaking, appears appropriate for decomposing risk and organizing information, and it has built models, data streams, and processes for executing risk analyses for some of its various missions. However, with the exception of risk analysis for natural disaster preparedness, the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested. Moreover, it is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses other than for natural disasters.

Recommendation: To develop an understanding of the uncertainties in its terrorism-related risk analyses (knowledge that will drive future im-

[22] The committee was informed at its meeting of November 2008 that the U.S. Coast Guard and Immigration and Customs Enforcement are also developing ERM processes that span just those component agencies, but the committee did not examine those processes.

provements), DHS should strengthen its scientific practices, such as documentation, validation, and peer review by technical experts external to DHS. This strengthening of its practices will also contribute greatly to the transparency of DHS's risk modeling and analysis. DHS should also bolster its internal capabilities in risk analysis as part of its upgrading of scientific practices.

The steps implied by this primary conclusion are laid out in the next chapter. The focus on characterizing uncertainties is of obvious importance to decision makers and to improving the reliability of risk models and analysis. The treatment of uncertainty is recognized as a critical component of any risk assessment activity (Cullen and Small, 2004; NRC, 1983, 1994, 1996, 2008; an overview is presented in Appendix A). Uncertainty is always present in our ability to predict what might occur in the future, and it is present as well in our ability to reconstruct and understand what has happened in the past. This uncertainty arises from missing or incomplete observations and data; imperfect understanding of the physical and behavioral processes that determine the response of natural and built environments and the people within them; subjectivity embedded within analyses of threat and vulnerability and in the judgments of what to measure among consequences; and our inability to synthesize data and knowledge into working models able to provide predictions where and when we need them.

Proper recognition and characterization of both variability and uncertainty are important in all elements of a risk assessment, including effective interpretation of vulnerability, consequence, intelligence, and event occurrence data as they are collected over time. Some DHS risk work reflects an understanding of uncertainties—for example, the uncertainty in the FEMA floodplain maps is well characterized, and the committee was told that TRAM can produce output with an indication of uncertainty (though this is usually suppressed in accordance with the perceived wishes of the decision makers and was not shown to the committee). However, DHS risk analysts rarely mentioned uncertainty to the committee, and DHS appears to be in a very immature state with respect to characterizing uncertainty and considering its implications for ongoing data collection and prioritization of efforts to improve its methods and models.

Closely tied with the topic of uncertainty is that of reflecting properly the precision of risk analyses. The committee saw a pattern of DHS personnel and contractors' putting too much effort into quantification and trusting numbers that are highly uncertain. Similarly, the committee observed a tendency to make risk analyses more complex than needed or justified. Examples were given earlier in this chapter with respect to TRAM and the Regional Resiliency Assessment Project in IP. Another example arose during the committee's site visit to IP, wherein a briefing provided examples of protective measures assigned by SMEs to different security features. For example, a high metal fence with barbed wire received a Protective Measure Index of 71, while a 6-foot wooden fence was given a PMI of 13. None of the DHS personnel could say whether the ratio

71/13 had any meaning with respect to vulnerability, yet the presentation continued with several graphics comparing the PMIs of various types of physical security measures as examples of the analyses provided by DHS. Another example comes from a presentation at the committee's first meeting on the National Maritime Strategic Risk Assessment, which included a Risk Index Number with four significant figures. These numbers are apparently used to compare different types of risk. There was no indication, however, that the National Maritime Strategic Risk Assessment relied on that false precision.

Uncertainty characterization cannot be addressed without clearer understanding (such as that obtained through documentation and peer review by technical experts external to DHS), strengthening of the internal skill base, and adherence to good scientific practices. Those topics are taken up in Chapter 5. The remainder of this chapter addresses other cross-cutting needs that are evident from the risk models and processes discussed above.

Comparing Risks Across DHS Missions

DHS is working toward risk analyses that are more and more comprehensive, in an attempt to enable the comparison of diverse risks faced by the department. For example, HSPD-18 directed DHS to develop an integrated risk assessment that covered terrorism with biological, chemical, radiological, and nuclear (CBRN) weapons. The next generation of TRAM is being developed to include the ability to represent a range of hazards—human-initiated, technological, and natural—and measure and compare risks using a common scale.[23] More generally, RMA created the Integrated Risk Management Framework in order to support disparate types of risk assessment and management within DHS and eventually across the homeland security enterprise.[24] The DHS Risk Steering Committee's vision for integrated risk management is as follows: "…to enable individual elements, groups of elements, or the entire homeland security enterprise to simultaneously and effectively assess, analyze, and manage risk from multiple perspectives across the homeland security mission space" (DHS-RSC, 2009).

The concept calls for risk to be assessed and managed in a consistent manner from multiple perspectives, specifically: (a) managed across missions within a single DHS component (e.g., within the Immigration and Customs Enforcement agency); (b) assessed by hazard type (e.g., bioterrorism or chemical terrorism); (c) managed by homeland security functions (e.g., physical and information-based screening of travelers and cargoes); and (d) managed by security domain (e.g., aviation security strategies) (DHS-RSC, 2009). If an approach

[23] Chel Stromgren (SAIC) presentation to the committee, November 24-25, 2008, Washington, D.C.
[24] Tina Gabbrielli (RMA) presentation to the committee, November 24-25, 2008, Washington, D.C.

to integrated risk management can be successfully developed and implemented, the opportunities for improving the quality and utility of risk analyses carried out by many components of DHS and by many partners should be extensive.

In the committee's view, this emphasis on integrated risk analyses is unwise given DHS's current capabilities in risk analysis and the state of the science. Integrated risk analysis collects analyses for all potential risks facing an entity, here DHS, and combines those risks into one complete analysis using a common metric. This is contrasted with comparative risk analysis which omits the last step. In comparative risk analysis, potential risks to the entity from many different sources are analyzed and the risks then compared (or contrasted), but no attempt is made to put them into a common metric. As previously noted, there are major differences in carrying out risk analyses for (1) natural disasters, which may rest on the availability of considerable amounts of historical data to help determine the threat (e.g., flood data derived from years of historical records produced from a vast network of stream gages, earthquake-related data concerning locations and frequency of occurrence of seismic disturbances), and (2) terrorist attacks, which may have no precedents and are carried out by intelligent adversaries resulting in a threat that is difficult to predict or even to conceptualize (e.g., biological attacks). Whereas natural disasters can be modeled with relative effectiveness, terrorist disasters cannot. A recent report by a group of experts concludes that it is simply not possible to validate (evaluate) predictive models of rare events that have not occurred, and unvalidated models cannot be relied upon" (JASON, 2009, p. 7).

The balancing of priorities between natural hazards and terrorism is far more than an analytic comparison of effects such as health outcomes. Political factors are major in such balancing, and these are affected by public and government (over)reaction to terrorism.

Even though many DHS components are using quantitative, probabilistic risk assessment models based to some extent on Risk = $f(T,V,C)$, the details of the modeling, and the embedded assumptions, vary significantly from application to application. Aggregation of the models into ones that purport to provide an integrated view is of dubious value. For example, NISAC sometimes manually integrates elements from the output of various models. There is large room for error when the outputs of one model serve as inputs for another. It might be wiser to build and improve CIKR interdependent systems simulation models by designing modules and integrating elements over time, rather than taking the current collection of models and "jamming them together." Decision support systems that provide risk analysis must be designed with particular decisions in mind, and it is sometimes easier to build new integrated models rather than trying to patch together a collection of risk models developed over time and for various purposes. A decision support system designed from the beginning to be integrated minimizes the chance of conflicting assumptions and even mechanical errors that can accrue when outputs are manually merged.

While corporations that practice ERM do integrate some risk models from across the enterprise and have developed disciplined approaches for managing

portfolios of risk, their risks are relatively homogeneous in character. They are not dealing with risks as disparate as the ones within the purview of DHS.

It is not clear that DHS recognizes the fundamental limitations to true integration. A working paper from DHS-RMA, "Terrorism Risk and Natural Hazard Risk: Cross-Domain Risk Comparisons" (March 25, 2009; updated July 14, 2009), concludes that "it is possible to compare terrorism risk with natural hazard risk" (p. 6). The working paper goes on to say that "the same scale, however, may be an issue" (p. 6). The committee agrees; however, it does not agree with the implication in the RMA paper (which is based on an informal polling of self-selected risk analysts) that such a comparison *should* be done. It is clear from the inputs of the polled risk analysts that this is a research frontier, not an established capability. There does not exist a general method that will allow DHS to compare risks across domains (e.g., weighing investments to counterterrorism risk versus those to prepare for natural disasters or reduce the risk of illegal immigration).

Even if one moves away from quantitative risk assessment, the problem does not disappear. There are methods in *qualitative* risk analysis for formally eliciting advice for decision making, such as Delphi analysis, scoring methods, and expert judgment, that can be used to compare risks of very different types. There is a well established literature on comparative risk analysis that can be used to apply the Risk = $f(T,V,C)$ approach to different risk types (Davies, 1996; EPA, 1987; Finkel and Golding, 1995). However, the results are likely to involve substantially different metrics that cannot be compared directly. However, the scope and diversity in the metrics can themselves be very informative for decision making.

Therefore, in response to element (d) of the Statement of Task, the committee makes the following recommendation:

Recommendation: The risks presented by terrorist attack and natural disasters cannot be combined in one meaningful indicator of risk, so an all-hazards risk assessment is not practical. DHS should not attempt an integrated risk assessment across its entire portfolio of activities at this time because of the heterogeneity and complexity of the risks within its mission.

The risks faced by DHS are too disparate to be amenable to quantitative comparative analysis. The uncertainty in the threat is one reason, the difficulty of analyzing the social consequences of terrorism is a second, and the difference in assessment methods is yet another. One key distinguishing characteristic is that in a terrorist event, there is an intelligent adversary intending to do harm or achieve other goals. In comparison, "Mother Nature" does not cause natural hazard events to occur in order to achieve some desired goal. Further, the intelligent adversary can adapt as information becomes available or as goals change; thus the likelihood of a successful terrorism event ($T \times V$) changes over time. Even comparing risks of, say, earthquakes and floods on a single tract of land raises difficult questions. As a general principle, a fully integrated analysis that

aggregates widely disparate risks by use of common metric is not a practical goal and in fact is likely to be inaccurate or misleading given the current state of knowledge of methods used in quantitative risk analysis. The science of risk analysis does not yet support the kind of reductions in diverse metrics that such a purely quantitative analysis would require.

The committee is more optimistic about using an integrated approach if the subject of the analysis is a set of alternative risk management options, for example, in an analysis of investments to improve resilience. The same risk management option might have positive benefits across different threats—for example, for both a biological attack and an influenza pandemic or an attack on a chemical facility and an accidental chemical release. In these cases, the same risk management option might have the ability to reduce risks from a number of sources such as natural hazards and terrorism. The analysis of the alternative risk management options that could mitigate risks to a set of activities or assets could be analyzed in a single quantitative model in much the same way that cost-effectiveness analysis can be used to select the least-cost investment in situation in which benefits are generally incommensurate. An example might be an analysis of emergency response requirements to reduce the consequences of several disparate risks.

Leading thinkers in public health and medicine have argued that preparedness and response systems for bioterrorism have the dual benefit of managing the consequences of new and emerging infections and food-borne outbreaks. Essential to management of both biological attacks and naturally occurring outbreaks is a robust public health infrastructure (Henderson, 1999; IOM, 2003). Among the shared requirements for outbreak response (whether the event is intentional or natural in origin) are a public health workforce schooled in the detection, surveillance, and management of epidemic disease; a solid network of laboratory professionals and diagnostic equipment; physicians and nurses trained in early detection of novel disease who are poised to communicate with health authorities; and a communication system able to alert the public to any danger and describe self-protective actions (Henderson, 1999; IOM, 2003).

Recent evidence supports this dual-use argument. State and local public health practitioners who have received federal grants for emergency preparedness and response over the past decade exhibit an enhanced ability to handle "no-notice" health events, regardless of cause (CDC, 2008; TFAH, 2008). Arguably, the additional epidemiologists and other public health professionals hired through the preparedness grants—the number of which doubled from 2001 to 2006—have improved the overall functioning of health departments, not simply their emergency capabilities (CDC, 2008). Hospitals, too, that have received federal preparedness grants originally targeted to the low-probability, high-consequence bioterrorist threat report an enhanced state of resilience and increased capacity to respond to "common medical disasters" (Toner et al., 2009). Among the gains catalyzed by the federally funded hospital preparedness program are the elaboration of emergency operation plans, implementation of communication systems, adoption of hospital incident command system con-

cepts, and development of memoranda of understanding between facilities for sharing resources and staff during disasters (Toner et al., 2009).

A parallel example can be found in managing the risks of hazardous chemicals. Improved emergency preparedness, emergency response, and disaster recovery can help contain the consequences of a chemical release, thus lessening the appeal of the chemical infrastructure as a target for terrorists. At the same time, such readiness, response, and recovery capabilities can better position a community to mitigate the effects of a chemical accident (NRC, 2006).

An NRC report (2006) that evaluated the current state of social science research into hazards and disasters noted that there has been no systematic scientific assessment of how natural, technological, and willful hazards agents vary in their threats and characteristics, thus "requiring different pre-impact interventions and post-impact responses by households, businesses, and community hazard management organizations" (p. 75). That report continued (NRC, 2006, pp. 75-76):

> In the absence of systematic scientific hazard characterization, it is difficult to determine whether—at one extreme—natural, technological, and willful hazards agents impose essentially identical disaster demands on stricken communities—or at the other extreme—each hazard is unique. Thorough examination of the similarities and differences among hazard agents would have significant implications for guiding the societal management of these hazards.

Recommendation: In light of the critical importance of knowledge about societal responses at various levels to risk management decisions, the committee recommends that DHS include within its research portfolio studies of how population protection and incident management compare across a spectrum of hazards.

It *is* possible to compare two disparate risks using different metrics, and that might be the direction in which DHS can head, but this requires great care in presentation, and there is a high risk that the results will be misunderstood. The metrics one applies to any one risk might be completely different from some other risk, and any attempt to squeeze them to fit on the same plot is likely to introduce too much distortion. Rather, the committee encourages *comparative risk analysis*[25] (which is distinct from *integrated or enterprise risk analysis*[26]) that is structured within a decision framework but without trying to force the risks onto the same scale.

One of the key assumptions in integrated or enterprise risk management (particularly for financial services firms) is that there is a single aggregate risk measure such as economic capital (Bank for International Settlements, 2006).

[25] See Davies, 1996; EPA, 1987; Finkel and Golding (ed.), 1995.
[26] See, for example, Committee of the Sponsoring Organizations of the Treadway Commission, 2004; Doherty, 2000.

Economic capital is the estimated amount of money that a firm must have available to cover ongoing operations, deal with worst-case outcomes, and survive. While many of the concepts of integrated or enterprise risk management can also be applied to DHS (particularly governance, process, and culture), there is currently no single measure of risk analogous to economic capital that is appropriate for DHS use. Thus, DHS must use comparative risk management—specifically multiple metrics to understand and evaluate risks. It is worth noting that most nonfinancial services firms implementing ERM adopt the philosophical concepts but have several metrics for comparative risk across operations. For example, nonfinancial services firms evaluate risks using comparative metrics such as time to recover operations, service-level impact over time, potential economic loss of product or service, number of additional temporary staffing (reallocated resources) to restore operations to normal levels, and other factors. These metrics are much more in line with DHS's needs to focus on response and recovery.

Comparative analysis works because the conceptual breakdown of risk into threat, vulnerability, and consequence can be applied to any risk. Rather than seeking an optimal balance of investments—and certainly rather than trying to do so through one complex quantitative model—DHS should instead use analytical methods to identify options that are adequate to various stakeholders and then choose among them based on the best judgment of leadership. It seems feasible for DHS to consider a broad collection of hazards, sketch out mitigation options, examine co-benefits, and develop a set of actions to reduce vulnerability and increase resilience. A good collection of risk experts could help execute a plan like that.

5
The Path Forward

Recommendation: To make progress incorporating risk analysis into the Department of Homeland Security (DHS), the committee recommends that the agency focus on the following five actions:

1. Build a strong risk capability and expertise at DHS.
2. Incorporate the Risk = *f*(*T*,*V*,*C*) framework, fully appreciating the complexity involved with each term in the case of terrorism.
3. Develop a strong social science capability and incorporate the results fully in risk analyses and risk management practices.
4. Build a strong risk culture at DHS.
5. Adopt strong scientific practices and procedures, such as careful documentation, transparency, and independent outside peer review.

BUILD A STRONG RISK CAPABILITY AND EXPERTISE AT DHS

Improve the Technical Capabilities of Staff

The Statement of Task for this study requires attention to staffing issues, to answer both element (b), regarding DHS's capability to implement and appropriately use risk analysis methods to represent and analyze risks, and element (c), regarding DHS's capability to use risk analysis methods to support DHS decision making. The right human resources are essential for effective risk analysis. The goal should be a strong, multi-disciplinary staff in the Office of Risk Management and Analysis (RMA), and throughout DHS, with diverse experience in risk analysis. Although RMA has made an effort to hire people with diverse backgrounds, most do not come to the office with previous experience in risk analysis.

As part of its responsibility in implementing the Integrated Risk Management Framework (IRMF), RMA could be spearheading DHS efforts to develop a solid foundation of expertise in all aspects of risk analysis. This stems in part from "Delegation 17001" from the DHS Secretary which, among other things, assigns RMA the responsibility of providing core analytical and computational capabilities to support all department components in assessing and quantifying risks.

The long-term success of risk analysis throughout DHS and the improve-

ment of scientific practice both depend on the continued development of an adequate in-house workforce of well-trained risk assessment experts. The need for technical personnel skilled in risk analysis throughout DHS should be addressed on a continuing basis. Decision support requires the ready availability of such resources, to ensure that specific risk assessments are carried out according to the appropriate guidelines and their results are clear to risk managers. Such a staff would also be responsible for the development and periodic revision of risk analysis guidelines. As DHS expands its commitment to risk analysis, personnel who are up to date on scientifically grounded methods for carrying out such analyses will be increasingly in demand. In the course of its study, the committee saw little evidence of DHS being aware of the full range of state-of-the art risk analysis and decision support tools, including those designed specifically to deal with deep uncertainty. Recruitment of additional personnel is clearly needed, and continuing education for personnel currently in DHS and working for contractors and personnel exchange programs between DHS and other stakeholders are also paths that should be followed.

To fully develop its capabilities for making strong risk-based decisions, DHS is critically dependent on staff with a good understanding of the principles of risk analysis who are thoughtful about how to improve DHS processes. DHS needs more such people; the lessons provided by the experience of the Environmental Protection Agency (EPA) and similar risk-informed agencies are instructive. At present, DHS is heavily dependent on private contractors, academic institutions, and government laboratories for the development, testing, and use of models; acquisition of data for incorporation into models; interpretation of results of modeling efforts; and preparation of risk analyses. While there are advantages in relying on external expertise that is not available within DHS, in-house specialists should be fully aware of the technical content of such work. In particular, they need to ensure the scientific integrity of the approaches and understand the uncertainties of the results that are associated with risk models and the products of these models. Contractor support will remain essential, but the direction of such work should be under the tight control of in-house staff. In-house staff would also provide the linkages with other agencies that are so critical to success and ensure that these interagency efforts are scientifically coordinated and appropriately targeted.

To truly become a risk-informed organization, DHS needs a long-term effort in recruiting and retaining people with strong expertise of relevance to the multidisciplinary field of risk management along with programs designed to build up a risk-aware culture. For example, there are pitfalls in the use of risk analysis tools (Cox, 2008). Sometimes they are minor, but other times they might invalidate the results. DHS needs some deep knowledge in risk analysis to guard against misapplication of tools and data and to ensure that its risk analysis produces valid information. The need to build up a risk-aware culture might very well extend to taking responsibility for training DHS partners in states, localities, tribal areas, territories, and owners and operators of Critical Infrastructure and Key Resources (CIKR) assets.

To offset the department's recognized shortage of risk analysis personnel, which was understandable when DHS was first established, it has elected to outsource a good deal of risk-related technical work. Other federal agencies have adopted the same strategy, but the approach has pitfalls, especially when work of a specialized technical character is outsourced. For example, it is difficult for agency staff to stay current in a technical discipline if they are not actively engaged in such work. Serving as a technical liaison is not enough to maintain or expand one's skill base. Sooner or later, DHS staff will find that they lack enough insight to sort through competing claims from contractors, choose the contractor for a given technical task, specify and guide the work, evaluate the work, and implement the results. Moreover, a paucity of skills at the program level can undercut the ability of senior leadership to make effective use of contractor work. In the case of two models reviewed by the committee, Biological Threat Risk Assessment (BTRA) and Terrorism Risk Assessment and Management (TRAM), it was not always clear that DHS leadership fully understood the fundamental scientific concerns with the risk analysis methodology chosen, the underlying assumptions used, the data inputs required, or how to use the analysis outputs.

Some risk models developed by DHS contractors remain proprietary, which introduces additional problems. How will DHS enable institutional learning if data management, models, and/or analysis capabilities are proprietary? In addition, proprietary work could slow the adoption and appropriate utilization of risk analysis models, methods, and decision support systems.

At present, DHS has a very thin base of expertise in risk analysis—many staff members are learning on the job—and a heavy reliance on external contractors. The Government Accountability Office (GAO) considers that DHS has significant organizational risk, due to the high volume of contractors in key positions supporting DHS activities, the higher-than-desired turnover of key DHS personnel, and a lack of continuity in knowledge development and transfer.[1] The committee agrees with that assessment. This combination of heavy reliance on contractors and a small in-house skill base also tends to produce risk-modeling tools that require a contractor's expertise and intervention for running and interpreting. This is an undesirable situation for risk management, which is most useful when the assumptions behind the model are transparent to the risk manager or decision maker and that person can directly exercise the model in order to explore "what-if" scenarios.

These concerns lead to the following recommendation:

Recommendation: DHS should have a sufficient number of in-house experts, who also have adequate time, to define and guide the efforts of external contractors and other supporting organizations. DHS' internal technical expertise should encompass all aspects of risk analysis, including the

[1] Tony Cheesebrough, GAO presentation to the committee. November 24, 2008, Washington, D.C.

social sciences. DHS should also evaluate its dependence on contractors and the possible drawbacks of any proprietary arrangements.

The committee recognizes that hiring appropriate technical people is difficult for DHS. Staff from both the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and RMA staff voiced frustration in recruiting technical talent, particularly those with advanced degrees and prior work experience across a wide variety of risk analysis fields, such as engineering disciplines, social sciences, physical sciences, public health, public policy, and intelligence threat analysis. Both units cited the longer lead times of 6-12 months required for security clearances and the DHS Human Resources process as limiting their ability to make offers and bring personnel on board in a time frame that is competitive with the private sector.

RMA has used the competitive Presidential Management Fellows Program to manage lead times in recruiting graduating M.S. and Ph.D. students. HITRAC works with key contractors to access technical staff while waiting for the DHS Human Resources recruiting process. Both RMA and HITRAC are actively educating job candidates and working on candidate communications to manage the longer lead times required in recruiting and signing technical talent. The committee hopes that DHS can improve its human resources recruiting process and close the time gap for recruiting top technical talent.

It is unlikely that DHS can fully develop strong risk-based decisions without such a staff; again, the lessons provided by the experience of EPA and similar agencies are instructive. Contractor support will remain essential, but the direction of such work should be under the tight control of in-house staff.

Such an in-house staff would also provide the linkages with other agencies that are so critical to success and ensure that those interagency efforts are scientifically coordinated and appropriately targeted.

Recommendation: DHS should convene an internal working group of risk analysis experts to work with its RMA and Human Resources to develop a long-term plan directed for the development of a multidisciplinary risk analysis staff throughout the department and practical steps for ensuring such a capability on a continuing basis. The nature and size of the staff and the rate of staffing should be matched to the department's long-term objectives for risk-based decision making.

DHS needs an office that can set high standards for risk analysis and provide guidance and resources for achieving those standards across the department. This office would have the mandate, depth of experience, and external connections to set a course toward risk analysis of the caliber that is needed for DHS's complex challenges. These challenges are putting new demands on the discipline of risk analysis, so DHS needs the capability to recognize best practices elsewhere and understand how to adapt them. This requires deep technical skill, with not only competence in existing methods but also enough insight to

discern whether new extensions are feasible or overoptimistic. It also requires strong capabilities in the practice of science and engineering to understand the importance of clear models, uncertainty estimates, and validation of models, and peer review and high-caliber outside advice to be able to sort through technical differences of opinion, and so on. The office that leads this effort must earn the respect of risk analysts throughout DHS and elsewhere. If RMA is to be the steward of DHS's risk analysis capabilities, it has to play by those rules and be an intellectual leader in this field. This will be difficult.

It is not obvious that RMA is having much impact: in conversations with a number of DHS offices and components about topics within risk analysis, RMA is rarely mentioned. This could simply reflect the fact that Enterprise Risk Management (ERM) processes generally aim to leverage unit-level risk with a light touch and avoid overlaying processes or otherwise exerting too much oversight. However, it could also be an indication that RMA is not adding value to DHS's distributed efforts in risk analysis.

Discard the Idea of a National Risk Officer

The director of RMA suggested to the committee that the DHS Secretary, who already serves as the Domestic Incident Manager during certain events, could serve as the "country's Chief Risk Officer." establishing policy and coordinating and managing national homeland security risk efforts.[2] A congressional staff member supported the concept of establishing a Chief Risk Officer for the nation.[3]

The committee has serious reservations.

Risk assessments are done for many issues, including health effects, technology, and engineered structures. The approaches taken differ depending on the issues and the agency requirements. The disciplinary knowledge required to address these issues ranges from detailed engineering and physical sciences to social sciences and law. For a single entity to wisely and adequately address this broad range would require a large—perhaps separate—agency. In addition, as other National Research Council (1989; 1996) studies have shown, risk analysis is best done with interactions between the risk analysts and stakeholders, including the involved government agencies. Obviously care must be taken not to have the analysis warped by pressures from the stakeholders, but interactions with stakeholders can improve the analysis. To be effective, such interactions require the federal agents to have an understanding of the issues and of the values of stakeholders (NRC, 1989). Each federal agency is responsible for this; some do it well, others poorly. However, to locate all in one agency and require the personnel to stay current is unlikely to succeed.

---

[2] RMA presentation to the committee, February 4-5, 2009, Washington D.C.

[3] Mike Beland, House Homeland Security Committee staff member, presentation to the committee. February 4-5, 2009, Washington, D.C.

In the previous administration, the White House Office of Management and Budget (OMB) attempted to develop a single approach to risk assessment to be used by all federal agencies. That effort was withdrawn following strong criticism by an NRC (2007b) report.

The President will be issuing a revision to Executive Order 12866, Regulatory Planning and Review.[4] This executive order may describe how risk assessment is to be done. It certainly will serve as guidance for some risk analysis. What a DHS office for a National Risk Officer could add is difficult to imagine. More likely such an office would lead to inefficiency and interminable bureaucratic arguments. DHS has been afflicted with shifting personnel and priorities. Neither would be of benefit in attempting to establish a single entity for risk management across all federal agencies.

Recommendation: Until risk management across DHS has been shown to be well coordinated and done effectively, it is far too premature to consider expanding DHS's mandate to include risk management in all federal agencies.

INCORPORATE THE RISK = *f*(*T*,*V*,*C*) FRAMEWORK, FULLY APPRECIATING THE COMPLEXITY INVOLVED WITH EACH TERM IN THE CASE OF TERRORISM

Even if DHS can properly characterize its basic data and has confidence in those data, the department faces a significant challenge in adopting risk analysis to support risk-informed decision making because there are many different tools, techniques, modeling approaches, and analysis methods to assess risk. *Quantitative risk analysis is not the only answer, and it is not always the best approach.* A good discussion of this is given in Paté-Cornell (1996). DHS should recognize that quantitative models are only one type of method and may not be the most appropriate for all risk situations.

Figure 5-1 shows a spectrum of more traditional risk analysis methods, from the more qualitative or subjective methods on the left to methods that rely heavily on data of high quality, volume, and objectivity on the right. The figure also attempts to capture the rapidly developing capabilities in modeling terrorism and intelligent adversaries, through tools such as attacker-defender (or defender-attacker-defender) models, game theory applied to terrorism, and systems or infrastructure network models and simulation. Given the type and amount of available input data and the type of decision to be made, the figure suggests which types of models and methods are available for risk analysis.

[4] Presidential memorandum of January 30, 2009—Regulatory Review—directed the director of OMB to produce a set of recommendations for a new executive order on Federal regulatory review. No further revision to Executive Order 12866 has been issued at the time this report went to press.

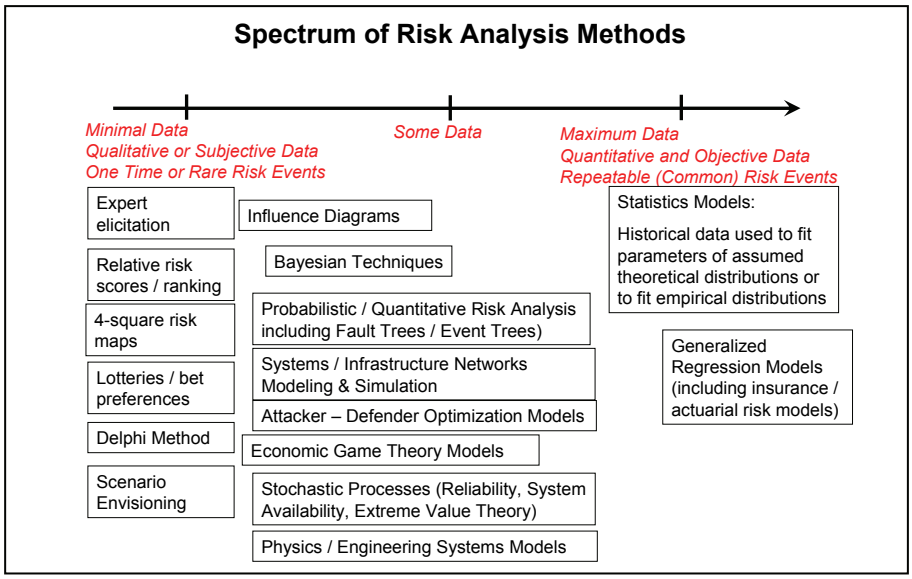

FIGURE 5-1 Spectrum of traditional risk analysis methods.

Rarely is there a single "right" risk analysis tool, method, or model to provide "correct" analysis to support decision making. In general, a risk analysis is intended to combine data and modeling techniques with subject matter expertise in a logical fashion to yield outputs that differentiate among decision options and help the decision maker improve his or her decision over what could be accomplished merely with experience and intuition. Such models can be used to gain understanding of underlying system behavior and how risk events "shock" and change the behavior of the system of interest; to evaluate detection, protection, and prevention options (risk-based cost-benefit analysis); or to simply characterize and compare the likelihood and severity of various risk events.

Many of the models and analyses reviewed by the committee treat chemical, biological, radiological, and nuclear (CBRN) terrorism and weapons of mass destruction (WMD) events as separate cases from natural hazards and industrial accidents. That may be because, in a quantitative assessment based solely on financial loss and loss of life, the risk of terrorist events tends to rank substantially lower than the risk of natural hazards and accidents. The quantitative assessments cannot capture the social costs of terrorism—the terror of terrorism.

A wide body of literature is available on appropriate methods for developing and applying technical models for policy analysis and decision support in a variety of disciplines (NRC, 1989, 1994, 1996, 2007d). The EPA, for example, provides support for environmental modeling in a number of its program and research offices, with a coordinated agency-wide effort led by the EPA Council for Regulatory Environmental Modeling (CREM) (*http://www.epa.gov/CREM/*

index.html). The purpose of the CREM is to

- Establish and implement criteria so that model-based decisions satisfy regulatory requirements and agency guidelines;
- Document and implement best management practices to use models consistently and appropriately;
- Document and communicate the data, algorithms, and expert judgments used to develop models;
- Facilitate information exchange among model developers and users so that models can be iteratively and continuously improved; and
- Proactively anticipate scientific and technological developments so EPA is prepared for the next generation of environmental models.

Of particular note to DHS, the EPA (2009) *Guidance Document on the Development, Evaluation and Application of Environmental Models* addresses the use and evaluation of proprietary models, which DHS relies on in some contexts:

> …To promote the transparency with which decisions are made, EPA prefers non-proprietary models when available. However, the Agency acknowledges there will be times when the use of proprietary models provides the most reliable and best-accepted characterization of a system. When a proprietary model is used, its use should be accompanied by comprehensive, publicly available documentation. This documentation should describe:
>
> - The conceptual model and the theoretical basis for the model.
> - The techniques and procedures used to verify that the proprietary model is free from numerical problems or "bugs" and that it truly represents the conceptual model.
> - The process used to evaluate the model and the basis for concluding that the model and its analytical results are of a quality sufficient to serve as the basis for a decision.
> - To the extent practicable, access to input and output data such that third parties can replicate the model results.
>
> *[Available online at: http:www.epa.gov/crem/library/cred_guidance_0309.pdf, pp. 31-34*]

Proprietary models used in DHS include at least the BTRA, the CTRA, and the Transportation Safety Administration's (TSA's) Risk Management Tool (RMAT). For those many areas where DHS models risk as a function of *T*, *V*, and *C*, the use of non-proprietary models would mean that the best models for each of these elements (*T*, *V*, and *C*) could be applied to the particular decision being addressed, rather than relying on one fixed risk model.

The DHS Risk Analysis Framework

In many cases, the DHS approach to risk analysis involves application of the simple framework that Risk = Threat × Vulnerability × Consequences (or $R = T \times V \times C$). As pointed out in the Congressional Research Service's 2007 report on Homeland Security Grant Program (HSGP), *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (Masse et al., 2007), this conceptual framework has evolved in that context through three stages of development: a first stage when risk was generally equated to population; a second stage when risk was, primarily in additive form, assessed as the sum of threat, critical infrastructure vulnerability, and population density. Finally, in stage 3, the current situation, the $R = T \times V \times C$ framework is used and the probability of threat events was introduced, although with unresolved issues (see below).

The general framework of $R = T \times V \times C$ builds upon accepted practice in risk assessment where, at its simplest level, risk has often been equated to the probability of events multiplied by the magnitude of expected consequences. The incorporation of vulnerability into this equation is entirely appropriate because it provides needed detail on how events lead to different types and magnitudes of consequences. In its 2005 review, the General Accounting Office evaluated the $R = T \times V \times C$ framework as containing the key elements required for a sound assessment of risk. The committee concurs with this judgment that *Risk = A Function of Threat, Vulnerability, and Consequences* (Risk = $f(T,V,C)$) is a suitable philosophical decomposition framework for organizing information about risks. Such a conceptual approach to analyzing risks from natural and man-made hazards is not new, and the special case of Risk = $T \times V \times C$ has been in various stages of development and refinement for many years. However, the committee concludes that the multiplicative formula, Risk = $T \times V \times C$, is not an adequate calculation tool for estimating risk for the terrorism domain, within which independence of threats, vulnerabilities, and consequences does not typically hold.

While the basic structure of the $R = f(T,V,C)$ framework is sound, its operationalization by DHS has been seriously deficient in a number of respects. In particular, problems exist with how each term of the equation has been conceptualized and measured, beginning with defining and estimating the probabilities of particular threats in the case of terrorism. The variables, indicators, and measures employed in calculating T, V, and C can be crude, simplistic, and misleading. Defining such threats and estimating probabilities are inherently challenging because of the lack of experience with such events, the associated absence of a database from which reliable estimates of probabilities may be made, and the presence of an intelligent adversary who may seek to defeat preparedness and coping measures. DHS has employed a variety of methods to compensate for this lack of data, including game theory, "red-team" analysis, scenario construction, and subjective estimates of both risks and consequences. Even here, however, these methods have often failed to use state-of-the-art methods,

such as the expert elicitation methods pioneered at Carnegie Mellon University. As a result, defining the full range of threats and their associated probabilities remains highly uncertain, a situation that is unlikely to change in the near term, even with substantial efforts and expenditures for more research and analysis. This reality seriously limits what can be learned from the application of risk assessment techniques as undertaken by DHS.

The DHS assessment of vulnerabilities has focused on critical infrastructure and the subjectively assessed likelihood that particular elements of critical infrastructure will become targets for terrorist attacks. The "attractiveness" of targets for terrorists, judged to provide a measure of the likelihood of exposure (i.e., likelihood it may be attacked), has been estimated by subjective expert opinion, including that of the managers of these facilities. However, this addresses only one of the three dimensions—exposure—that are generally accepted in risk analysis as contributing to vulnerability. The other two dimensions, coping capacity and resilience (or long-term adaptation), are generally overlooked in DHS vulnerability analyses. So the DHS program to reduce the nation's vulnerabilities to terrorist attack has focused heavily on the "hardening of facilities."

This tendency to concentrate on hardware and facilities and to neglect behavior and the response of people remains a major gap in the DHS approach to risk and vulnerability. This omission results in a partial analysis of a complex problem.

Uncertainty and variability analyses are essential ingredients in a sound assessment of risk. This has most recently been pointed out at length in the recent NRC 2009 report *Science and Decisions: Advancing Risk Assessment*. There is also general consensus in the field of risk analysis on this issue. This is a particularly important issue in DHS risk-related work, especially for terrorism, where uncertainty is particularly large. As many authoritative studies have noted, it is essential to assess the levels of uncertainty associated with components of the risk assessment and to communicate these uncertainties forthrightly to users and decision makers. Regrettably, this has not been achieved in much of the DHS analysis of risk. Instead of estimating the types and levels of uncertainty, DHS has frequently chosen to weight heavily its consequence analyses, where magnitudes of effects can be more easily estimated, and to reduce the weight attached to threats, where the uncertainties are large. This is not an acceptable way of dealing with uncertainty. Rather, the large uncertainties associated with the difficult problem of threat assessment should be forthrightly stated and communicated. It would be helpful to have further assessment of the types of uncertainty involved, to differentiate between those that can be reduced by further data gathering and research and those that lie in the domain of "deep uncertainty," where further research in the near term is unlikely to change substantially the existing levels of uncertainty. Sensitivity analyses tied to particular risk management strategies could help identify which types of data would be most important.

Even a sound framework of risk leaves unresolved what the decision rule should be for combining terms into an integrative, or multidimensional, metric

of risk. In the risk field, it is commonly assumed that the terms should be unweighted unless there is compelling evidence to support a weighting process, and that the terms should be multiplied by each other. In DHS applications, it is unclear how risk is to be calculated. Sometimes terms are multiplied; other times they are added. These give essentially inconsistent and incomparable end results about risk. A coherent and consistent process needs to be developed to which all assessments adhere.

Conclusions:

1. The basic risk framework of Risk = *f* (*T*,*V*,*C*) used by DHS is sound and in accord with accepted practice in the risk analysis field.

2. DHS' operationalization of that framework—its assessment of individual components of risk and the integration of these components into a measure of risk—is in many cases seriously deficient and is in need of major revision.

3. More attention is urgently needed at DHS to assessing and communicating the assumptions and uncertainties surrounding analyses of risk, particularly those involved with terrorism.

Until these deficiencies are improved, only low confidence should be placed in most of the risk analyses conducted by DHS.

The FY 2009 Homeland Security Grant Guidance describes the DHS approach to risk assessment as (DHS, 2009):

> Risk will be evaluated at the Federal level using a risk analysis model developed by DHS in conjunction with other Federal entities. Risk is defined as the product [emphasis added] of three principal variables:
>
> *Threat*—the likelihood of an attack occurring
> *Vulnerability*—the relative exposure to an attack
> *Consequence*—the expected impact of an attack

The committee says that DHS "tends to prefer" the definition Risk = $T \times V \times C$ because it is unclear whether that formula is followed in the grants program: that program's weighting of threat by 0.10 or 0.20 doesn't make sense unless some other formulation is used.[5] Moreover, committee discussions with staff from Office of Infrastructure Protection (IP) and National Infrastructure Simulation and Analysis Center (NISAC) illuminated how *T*, *V*, and *C* are assessed, but there does not seem to be a standard protocol for developing a measure of risk

[5] Following Cox (2008), weighted values are *probably* evaluated through the expedient of calculating the log of the risk and weighting the logs of the components of risk: $R = T \times (VC)$ is rewritten as $\log(R) = \log(T) + \log(VC)$. Then the weighting is effected as $\log(R) = 0.2 \times \log(T) + 0.8 \times \log(VC)$. Exponentiation can retrieve the estimate of risk.

from those component assessments. RMA defines risk in the DHS Risk Lexicon as "the potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence [emphasis added]" (DHS-RSC, 2008).

The definition Risk = $T \times V \times C$ makes sense when T, V, and C are independent variables—in particular, when threat is independent of vulnerabilities and consequences, as is the case for natural hazards. The formulation assumes this independence; for example, the threat against a given facility does not change if its vulnerability goes up or the consequences of damage increase, although the overall risk to that facility will increase in either case. Given the independence of T, V, and C, the procedure for making a multiplicative assessment of risk is relatively straightforward as long as the probabilities can be estimated with some confidence and the consequences evaluated on some type of consistent metric. However, to state the obvious; a terrorist would be attracted by a soft target, whereas while a storm strikes at random. Also, vulnerability and consequences are highly correlated for terrorism but not for natural disasters. Intelligent adversaries exploit these dependencies. Challenges exist in any instance where T, V, and C are poorly characterized, which can be the case even with the risk of natural disasters and accidents. Yet this is the normal state with regard to terrorism, where T tends to be very subjective and not transparent, V is difficult to measure, and we do not know how to estimate the full extent of consequences.

Multiattribute utility theory (as used in economics and decision analysis) is one way to combine multiple attributes into a single metric for a single decision maker with a unique set of preferences. However, Arrow's impossibility theorem (Arrow, 1950) shows that there is no unique consensus way to combine different attributes in "group" decision theory when the members of the group have different priorities or weights on the various attributes. (In other words, the relative importance of different attributes is a political question, not a scientific question.) So even if we had reliable methods of risk analysis for terrorism, those methods would not in general yield a unique ranking of different terrorist threats; rather, different rankings would result, depending on the weights placed on the attributes by particular stakeholders. (In addition, utility theory might not work well for events with extremely large consequences and extremely small probabilities.) Risk methods should not prejudge the answers to trade-off questions that are inherently political or preclude input by decision makers and other stakeholders.

Based on these concerns, the committee makes the following recommendations:

Recommendation: DHS should rapidly change its lingua franca from "Risk = $T \times V \times C$" to "Risk = $f(T,V,C)$" to emphasize that functional interdependence must be considered in modeling and analysis.

Recommendation: DHS should support research into how best to combine T, V, and C into a measure of risk in different circumstances. This

research should include methods of game theory, Bayesian methods, red teams to evaluate *T*, and so on. The success of all approaches depends on the availability and quality of data.

DEVELOP A STRONG SOCIAL SCIENCE CAPABILITY AND INCOPORATE THE RESULTS FULLY IN RISK ANALYSES AND RISK MANAGEMENT PRACTICES

A particular concern of the committee's is an apparent lack of expertise in social sciences, certainly in RMA, but apparently also in other DHS units responsible for risk analysis. Social science expertise is critical to understand terrorism risk and to properly model societal responses to any type of hazardous scenario, and this absence poses a major gap in DHS expertise. Other kinds of social science expertise are fundamental to developing and guiding reliable expert elicitation processes, which are essential to the success of DHS risk analysis and to designing and executing effective programs of risk communication that take into account public perception and societal responses. The Study of Terrorism and Response to Terrorism (START) Center of Excellence supported by DHS-S&T (Science and Technology Directorate) has expertise in understanding terrorism risk, but the committee saw no evidence that that expertise was influencing the thinking of DHS personnel dealing with risk analysis. The Center for Risk and Economic Analysis of Terrorism Events (CREATE) Center of Excellence has apparently had more impact—for example, it helped strengthen the expert elicitation processes used for the BTRA—but otherwise its work seems to have little effect on DHS risk analysis. Neither the Centers of Excellence nor S&T's Human Factors Division is devoting large amounts of effort into the two areas discussed next, understanding societal responses and risk communication. Without this expertise—and especially without knowledge of these areas being front and center in the minds of DHS risk analysts—it is unlikely that DHS will attain its goals for being an effective risk-informed organization.

Social Science Skills Are Essential to Improving Consequence Modeling

The range of possible consequences for some types of terrorism attacks and natural disasters can vary over several orders of magnitude. For example, exactly the same scenario can result in only a few fatalities or thousands, depending on when and how the event unfolds, the effectiveness of the emergency response, and even random factors such as wind direction. The latter factors—for example effectiveness of response and wind direction—also affect the consequences associated with natural hazards; yet an intelligent adversary will select the conditions that maximize consequences, to the degree that he or she can, and

thus the analyst's ability to estimate those consequences may be much poorer than in the case of natural hazards. However, many methods in routine use by DHS require an analyst to provide a single point estimate of consequences or at least a single category of consequence severity. This can easily lead to misleading results, especially if the decision maker's preference (i.e., utility function) is nonlinear in the relevant consequence measure—which might well be the case. This is not inherently a daunting problem for risk analysis, because rigorous methods exist for performing uncertainty analysis, even with extremely broad probability distributions for consequences. However, these methods might not be cost-effective for use in widespread application. Also, the probability distributions for consequences might be difficult to assess based on expert opinion, especially on a routine basis for large numbers of problems, by analysts with moderate levels of capability and resources.

In two specific cases examined by the committee (infrastructure protection and TRAM), DHS's consequence modeling is in general too limited in what it considers. That is not always wrong for a particular stakeholder's needs, but it is misleading if the modeling should illuminate the full extent of homeland security risk.

For example, social disruption is probably a common goal for terrorists, but the committee did not see any consequence analysis at DHS that includes this. In fact, it encountered few, if any, DHS staffers who seem concerned about this gap. What DHS is doing now is not necessarily wrong (and its decisions might be robust enough despite the coarseness of this approach), but DHS should be aware that important factors are being overlooked.

Immediately following 9/11 and the nearly concurrent mailings of the anthrax letters, U.S. government agencies and the government and nongovernmental scientific communities expanded many of their research efforts to focus on (1) the psychological impacts of terrorist attacks on people and (2) the short- and long-term economic consequences of such attacks. With the disruptions following Hurricane Katrina, the need to improve understanding of the responses of affected populations to natural disasters also received a new emphasis within government in anticipation of future catastrophic events. These three experiences were important wake-up calls to the broad scope of the consequences of disasters.

Such consequences include not only destruction over large geographic areas but also disruptions to sprawling social networks and multifaceted economic systems within and beyond the geographic impact zones. In addition to resulting in bodily harm, such incidents can indirectly devastate the lives of other individuals who are not killed or physically injured during the events (see, for example, Chapters 9 to 11 of NRC, 2002), and the consequences can affect the entire national economy.

Of particular concern are the shortcomings in labeling those persons directly affected by such events as the "public," which is then too often considered by the government as a homogeneous entity. Different groups are affected in different ways. Prior personal experiences, which vary from individual to indi-

vidual, are important. The resilience of members of the affected population to cope with tragedy varies significantly, and their personal prior experiences cannot easily be aggregated in a meaningful fashion. Among significant differentiating factors are previous experiences in dealing with disasters, types of education, levels of confidence in government plans for coping with disasters, availability of personal economic resources for recovery activities, and attachments of residents to the physically affected geographical areas and facilities through family, professional, and social networks.

Behavioral and emotional responses to natural disasters and terrorist attacks are difficult to predict because there are so many scenarios, each with its own set of impacts that condition the nature of the responses. Examples of responses to terrorist attacks include the following: fear of additional attacks, outrage calling for retaliation, lack of confidence in government to provide protection, proactive steps by neighbors to assist one another, eagerness to leave an affected area, and so on. Similarly with regard to natural disasters, a variety of responses could ensue, perhaps driven by lack of trust in the government—apprehensions as to personal economic losses, frustrations associated with evacuation planning and implementation, and lack of communication about the safety of families and friends. There has been considerable research in this area (see, e.g., Mileti, 1999 and Slovic, 2000, 2002).

In regard to consequence assessment, a perennial problem in risk analysis is the question of completeness: What are the consequence of concern to decision makers and publics? A recent NRC report on radiological terrorism in Russia identified as a major issue the need for "a risk-based methodology that considers the psychological consequences and economic damage of radiological terrorism as well as the threat to human life and human health. (NRC, 2007e)." This same need should be recognized as a major one for DHS because it has often been observed that a primary purpose, if not *the* primary purpose, of terrorism is to produce a sense of terror in the population. Clearly, social disruption is an essential part of any sound consequence analysis of terrorism. Personnel at several DHS Centers of Excellence are certainly attuned to this. Yet, despite that, the almost exclusive concentration among DHS risk analysts is on damage to critical infrastructure and the need to "harden" facilities, leaving this important domain of consequences unassessed. Accordingly, the partial approach to risk analysis employed at DHS carries the risk that DHS is working on the wrong problems, because terrorists might be aiming for an entirely different set of consequences than those that are driving DHS priorities.

As to economic impacts, 9/11 demonstrated the far-reaching effects of damage in a central financial district. Significant costs were felt by the U.S. economy, both through business losses attributable to the attack and also due to the hundreds of billions of dollars spent to harden facilities across the country. While such a huge expenditure is unlikely in the future, any attack will certainly trigger unanticipated government expenditures to prevent repetition and will disrupt businesses that depend in part on unencumbered activities in the impact zone.

From the outset of the establishment of DHS, a number of components of the department have been involved in efforts to reduce the adverse social and economic consequences of disasters over a broad range of impacts. The Federal Emergency Management Agency (FEMA), for example, has an array of programs to respond to the needs of affected populations. DHS's Science and Technology Directorate has established a program to support research in the behavioral sciences through a Human Factors Division and several university Centers of Excellence. This research is devoted to understanding the nature of the terrorist threat, designing measures to reduce the likelihood of successful attacks, and providing guidance in responding to the needs of populations affected by terrorist attacks or natural disasters (DHS-S&T, 2009). As a third example, the Office of Infrastructure Protection works closely with the private sector to minimize the economic disruption that follows disasters, whether naturally occurring or attributable to terrorist attacks (DHS-IP, 2009).

At the same time, however, DHS clearly gives much higher priority to hardening physical infrastructures (e.g., critical buildings and transportation and communications systems) than to preparing society on a broader basis to better withstand the effects of disasters. An important reason for this lack of balance in addressing consequences is that DHS has not devoted sufficient effort to the development of staff capabilities for adequately assessing the significance of the broad social and economic dimensions of enhancing homeland security.

DHS is in the early stages of embracing social and economic issues as major elements of homeland security. This belated development of capabilities in the social and economic sciences should be strongly encouraged. An increased reliance on such capabilities can upgrade DHS efforts to use quantitative modeling for anticipating a broader range of consequences of catastrophic events than in the past, particularly those consequences that lead to large-scale social and economic disruptions.

To improve preparations for managing a broad range of consequences, quantitative risk analyses should take into account the diverse ramifications to the extent possible. Of course, such estimates are inherently difficult; many new scenarios will have no precedents. More common scenarios might have different impacts in different geographic settings. Often there are difficulties in conceptualizing social and economic impacts, let alone characterizing the details of the consequences of an event. Nevertheless, these aspects of risk analysis must be recognized because in some cases, particularly with terrorism, social and economic impacts can be more significant than physical destruction and even loss of life.

There are many gaps in our ability to estimate short-term and long-term social and economic impacts of natural disasters and terrorism attacks. However, researchers have made good progress in recent years in the quantification of social and economic issues.[6] Those results should be used in modeling efforts within DHS. Considerable data concerning consequences are available to help

[6] For example, Bier and Azaiez (2009), Bier et al. (2007, 2008), Cox (2009), NRC (2002).

in validating efforts to model the consequences of disasters. Incorporating such considerations in pre-event planning and response preparedness should pay off when events occur.

Recommendation: DHS should have a well-funded research program to address social and economic impacts of natural disasters and terrorist attacks and should take steps to ensure that results from the research program are incorporated into DHS's risk analyses.

Recommendation: In characterizing risk, DHS should consider a full range of public health, safety, social, psychological, economic, political, and strategic outcomes. When certain outcomes are deemed unimportant in a specific application, reasons for omitting this aspect of the risk assessment should be presented explicitly. If certain analyses involve combining multiple dimensions of risk (e.g., as a weighted sum), estimates of the underlying individual attributes should be maintained and reported.

Social Science Skills are Essential to Improving Risk Communication

Element (d) of the Statement of Task calls for the committee to "make recommendations for best practices, including outreach and communications." In the large, highly dispersed domain of actors with which DHS deals, and with diverse publics who may be at risk, risk communication is a critical part of the DHS risk management program. Assembling and sharing common information are essential for coherent risk management. Indeed, DHS recognizes this in its IRMF, which identifies the critical DHS need to "develop information-sharing structures and processes that make risk information available among components and at the enterprise level, when and where it is required." The DHS focus since its inception has been on information sharing with decision makers. However, there is a much bigger job to be done to provide not only information but analysis and aids to thinking that prepare those who may be at risk to cope better with risk events that may occur. Those at risk are very diverse—tribal members, urban dwellers, state officials, and others. A concerted effort to prepare various publics for risk events has yet to be forthcoming, although aspects of needed work have been accomplished, such as producing a lexicon for risk terminology that should lessen the risk of confusion in information sharing. As DHS moves to the next stages of risk communication—which will have to go far beyond information sharing and include understanding the perceptions and needs of the recipients of various risk-related communications so that the messages can be tailored to fit the audiences—a well-developed risk communication strategy document and program, adequately staffed and funded, will be needed.

Recommendation: The DHS risk communication strategy and program must treat at minimum the following:

- **An identification of stakeholders and those at risk who need information and analysis;**
- **An assessment of the needs of these people to be met by the communication program (sometimes termed, Who are the audiences?);**
- **Strategies for two-way communication with these groups;**
- **Ongoing evaluation of program effectiveness and needed strategy changes;**
- **Learning from experience as events occur and changes in communication are suggested;**
- **Links between communications and actions people can take; and**
- **Outcomes resulting—cost and time considerations.**

The program should be developed with careful involvement of national experts and with external peer review. It should be accompanied, indeed anticipated, by public perception research.

Effective risk communication is quite difficult. It should be done by staff who understand the issues and details of the risk analyses. This is not public relations work, as some may believe, but work that requires participation by technically knowledgeable staff. DHS does not seem to understand the lessons painfully learned by other agencies, such as the Department of Energy (DOE), EPA, and the Nuclear Regulatory Commission.

In developing best practices for communicating risk, DHS should understand four audiences: DHS employees, other federal employees, members and staff of Congress, and the general public. The knowledge bases and information needs of these audiences differ, although the fundamental principles of risk communication apply to all. Another important aspect of DHS responsibilities—but beyond the domain of risk analysis—is communication during emergencies.

A 1989 NRC report, *Improving Risk Communication* recommended the following best practices:

- Relate the message to the audiences' perspectives: "risk messages should closely reflect the perspectives, technical capacity, and concerns of the target audiences. A message should (1) emphasize information relevant to any practical actions that individuals can take; (2) be couched in clear and plain language; (3) respect the audience and its concerns; and (4) seek to inform the recipient …. One of the most difficult issues in risk communication in a democratic society is the extent to which public officials should attempt to influence individuals …".
- "Risk message and supporting materials should not minimize the existence of uncertainty. Some indication of the level of confidence of estimates and the significance of scientific uncertainty should be conveyed."

- "Risk comparisons can be helpful, but they should be presented with caution. Comparison must be seen as only one of several inputs to risk decisions, not as the primary determinant" (pp 11-12).
- "Risk communication should be a two-way street. Organizations that communicate risk should ensure effective dialogue with potentially affected outsiders … [T]hose within the organization who interact directly with outside participants should be good listeners" (pp. 151, 153).

Other good sources on this topic include Bennett and Calman (1999) and Pidgeon et al. (2003). Effective risk communication relies on the involvement of competent people who understand the activities about which they speak.

It is worth noting that DHS has adopted a National Strategy for Information Sharing (DHS, 2008). This is fine as far as it goes, but it has to go much deeper into the issues of stakeholder and public needs, as suggested above. Recognition is also needed that the communication issues associated with terrorism and natural hazards are fundamentally different and will require quite different approaches, both in preparedness and in emergency response.

BUILD A STRONG RISK CULTURE AT DHS

The committee is concerned about the lack of any real risk analysis depth at DHS or in RMA and does not see this situation improving in recent hiring or training programs.

The challenges in building a risk culture in a federal agency or corporation are major, requiring a serious effort. At the DuPont Corporation, for example, this involved high-level commitment, diffusion of values throughout the corporation, routines and procedures, recruitment of people, and reward structures. It was not clear to the committee whether DHS has any serious plan for how this will happen and any serious ongoing evaluation of progress.

DHS would find benefit from many of the recommendations offered over the past 25 years to the EPA and other federal agencies that rely on risk analysis, as well as study of the practices that the EPA, in particular, has put into place to implement them. Of particular importance is the need for DHS to specify with complete clarity the specific uses to which risk analysis results will be put. This echoes the first recommendation of the NRC's 2007 *Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis*, which called for DHS to "establish a clear statement of the long-term purposes of its bioterrorism risk analysis" (NRC, 2007c):

> A clear statement of the long-term purposes of the bioterrorism risk analysis is needed to enunciate how it can serve as a tool to inform risk assessment, risk perception, and especially risk-management decision making. Criteria and measures should be specified for assessing how well these purposes are achieved. Key issues to be addressed by such

> a statement should include the following: who the key stakeholders are; what their short- and long-term values, goals, and objectives are; how these values, goals, and objectives change over time; how the stakeholders perceive the risks; how they can communicate their concerns about these risks more effectively; and what they need from the risk assessment in order to make better (more effective, confident, rational, and defensible) resource-allocation decisions. Other important issues are who should perform the analyses (contractors, government, both) and how DHS should incorporate new information into the analyses so that its assessments are updated in a timely fashion.

As part of its effort to build a risk culture and also improve its scientific practices (see next section), DHS should work to build stronger two-way ties with good academic programs in risk analysis of all types. To address these needs, DHS could develop programs that encourage its employees to spend a semester at one of the DHS university Centers of Excellence in order to strengthen their skills in a discipline of relevance to homeland security. Such a program should be bilateral in the sense that students at those Centers of Excellence should also be encouraged to spend time at DHS, either in rotating assignments or as employees after graduation. The goal is to implement technology transfer, from universities to the homeland security workforce, while keeping those universities grounded in the real needs of DHS. Improving risk modeling at DHS will require commensurate building up of academic ties, training of DHS people, and tech transfer routes to the DHS user community.

RMA and Enterprise Risk Management

Enterprise Risk Management as a field of management expertise began in the financial services sector in the late 1990s and is still evolving rapidly. Chapter 2 gives an introduction to ERM and explains how RMA is working to develop the three dimensions of a successful ERM system—governance, processes, and culture—with its Integrated Risk Management Framework. Generally speaking, RMA's primary focus has been on processes—facilitating more coherence across the preexisting risk practices within DHS components—and this is appropriate. Its development of a risk lexicon and an interim IRMF are reasonable starting points in the process, although the committee believes that the IRMF must be made more specific before it begins to provide value. Creating an inventory of risk models and risk processes throughout the department was also a logical and necessary early step. RMA's primary action in support of ERM governance was the establishment of the Risk Steering Committee. RMA has done little to date to help establish a risk-aware culture within DHS, although its existence and activities represent a beginning.

A central tenet of ERM—almost a tautology—is that it be driven from the top. An enterprise's top leadership must first show itself to be fully supportive of ERM, so that ERM practices are seen as fundamental to the organization's

mission and goals. That has been done at DHS, with both Secretary Chertoff and Secretary Napolitano emphasizing the centrality of risk-informed decision making to the department's success. For example, Secretary Napolitano included the following in her terms of reference for the 2009 Quadrennial Homeland Security Review:

> Development and implementation of a process and methodology to assess national risk is a fundamental and critical element of an overall risk management process, with the ultimate goal of improving the ability of decision makers to make rational judgments about tradeoffs between courses of action to manage homeland security risk.

Other federal organizations that have mature risk cultures and processes, such as the EPA and Nuclear Regulatory Commission, took years or decades to mature. It seems likely that the development of a mature risk culture at DHS will similarly require time, and DHS should attempt to learn from the experience of other departments and agencies that have trod the path before. Even though there has been relative success of risk management in the corporate world, DHS should not necessarily naively adopt best practices in risk management from industry. Risk management in financial services and insurance relies on some key assumptions that do not necessarily hold for DHS. For example, the law of large numbers may not hold for DHS, precisely because DHS does not get to observe millions of risk events, as would be available in auto insurance losses or financial instrument trades. Further, the financial services and insurance sectors rely on being able to collect and group data into relatively homogeneous groups and to have independence of risk events. DHS often has heterogeneous groups, and independence certainly does not hold for interdependent CIKR sectors or networks of operations.

Even the cultural best practices of risk management from the private sector need to be modified for DHS adoption. Losses occur in the private sector but not on the magnitude of DHS's decision scale, and not with the nonfinancial consequences that DHS must consider in managing risk. Societal expectations of DHS are vastly different from those of an investment firm, and many more stakeholder perspectives must be taken into account by DHS in managing risks. Lastly, the private sector relies on making decisions under uncertainty and adapting strategy and tactics over time as the future becomes clearer. Congress should expect DHS to demonstrate adaptive learning over time to address and better manage the ever-changing portfolio of homeland security risks.

ADOPT STRONG SCIENTIFIC PRACTICES AND PROCEDURES, SUCH AS CAREFUL DOCUMENTATION, TRANSPARENCY, AND INDEPENDENT OUTSIDE PEER REVIEW

Develop Science-Based Guidelines for Different Types of DHS Risk Analyses

A key tool, which could be of value to DHS, would be peer-reviewed guidelines that spell out not only how different types of risk analysis are to be carried out, but also which decisions those analyses are meant to inform. Clear, science-based guidelines have contributed greatly to the success of the U.S. Environmental Protection Agency in developing capabilities, over a 20-year period, for using risk analysis to inform strategic decision making and decisions about risk reduction. Such guidelines, when well developed, provide both the scientific basis for methods and guidance on the sources and types of data needed to complete each type of analysis. See Appendix B for a general discussion of how risk analysis evolved at EPA.

EPA has invested heavily in the development of its guidelines. Fundamental building blocks for this success include the development of clear characterization of the kinds of decisions that must be addressed by risk analysis, clear understanding about how to address each kind of decision, and an understanding of how to treat uncertainties in both data and models. (Appendix A contains background on uncertainty characterization.) EPA also has a strong focus on transparency, providing clear documentation of how it moves from risk analysis to decisions, and it has developed a fairly clear taxonomy of decisions. To enable these steps, EPA has developed a large professional staff that supports the guidelines by, for example, tracking the literature and continually improving the guidelines. The development of guidelines is based heavily on the published (primary) scientific literature, with gaps in that literature fully discussed to provide guidance for future research. Peer review is essential before guidelines are accepted for use.

Development of these guidelines should be preceded by elucidation of the specific types of risk-based decisions that the department is required to make and identification of the types of risk assessments most useful for those decisions. Guidelines should include the scientific bases, drawn from the literature, for the methods used and full discussion of the sources and types of data necessary to complete an assessment. Guidance on how uncertainties are to be treated should be central to the guidelines. Guidelines should be implemented only after they have been subjected to independent peer review. The ways in which the results of risk assessment support decisions should always be explicitly described.

While DHS is developing some guidelines for risk analysis (as addenda to the Integrated Risk Management Framework), they do not have the focus rec-

ommended here.

Recommendation: DHS should prepare scientific guidelines for risk analyses recognizing that different categories of decisions require different approaches to risk analysis strict reliance on quantitative models is not always the best approach.

The committee suggests as a starting point the development of specific guidelines for how to perform reliable, transparent risk analyses for each of the illustrative risk scenarios (Table 5-1) that have been adopted by DHS to help guide the efforts to address such scenarios.

Improve Scientific Practice

The charge for this study was to evaluate how well DHS is doing risk analysis. DHS has not been following critical scientific practices of documentation, validation, peer review, and publishing. Without that discipline, it is very difficult to know precisely how DHS risk analyses are being done and whether their results are trustworthy and of utility in guiding decisions.

As illustrated in the sections on uncertainty and avoiding false precision in Chapter 4 and in the discussion about how *T*, *V*, and *C* are combined to measure risk in different circumstances, it is not easy to determine exactly what DHS is doing in some risk analyses because of inadequate documentation, and the details can be critical for determining the quality of the method. It is one thing to evaluate whether a risk model has a logical purpose and structure—the kind of

TABLE 5-1 National Planning Scenarios

Scenario 1:	Nuclear Detonation—Improvised Nuclear Device
Scenario 2:	Biological Attack—Aerosol Anthrax
Scenario 3:	Biological Disease Outbreak—Pandemic Influenza
Scenario 4:	Biological Attack—Plague
Scenario 5:	Chemical Attack—Blister Agent
Scenario 6:	Chemical Attack—Toxic Industrial Chemicals
Scenario 7:	Chemical Attack—Nerve Agent
Scenario 8:	Chemical Attack—Chlorine Tank Explosion
Scenario 9:	Natural Disaster—Major Earthquake
Scenario 10:	Natural Disaster—Major Hurricane
Scenario 11:	Radiological Attack—Radiological Dispersal Devices
Scenario 12:	Explosives Attack—Bombing Using IED
Scenario 13:	Biological Attack—Food Contamination
Scenario 14:	Biological Attack—Foreign Animal Disease
Scenario 15:	Cyber Attack

information that can be conveyed through a briefing—but quite another to really understand the critical inputs and sensitivities that affect implementation. The latter understanding comes from scrutiny of the mathematical model, evaluation of a detailed discussion of the model implementation, and review of some model results, preferably when exercised against simple bounding situations and potentially retrospective validation. Good scientific practice for model-based scientific work includes the following:

- Clear definition of model purpose and decisions to be supported;
- Comparison of the model with known theory and/or simple test cases or extreme situations;
- Documentation and peer review of the mathematical model, generally through a published paper that describes in some detail the structure and mathematical validity of the model's calculations; and
- Some verification and validation steps, to ensure that the software implementation is an accurate representation of the model and that the resulting software is a reliable representation of reality.

In the absence of these steps, one cannot assess the quality and reliability of the risk analyses. As noted above, it is not adequate to simply ask subject matter experts (SMEs) whether they see anything odd about the model's results. DHS has generally done a poor job of documenting its risk analyses. The NRC committee that authored the BTRA review could really understand what the software was doing only by sitting down with the software developers and asking questions. No description has ever been published. That committee's report includes the following characterization (NRC, 2008, p. 37):

> The committee also finds the documentation for the model used in the BTRA of 2006 to be incomplete, uneven, and extremely difficult to understand. The BTRA of 2006 was done in a short time frame. However, deficiencies in documentation, in addition to missing data for key parameters, would make reproducing the results of the model impossible for independent scientific analysis. For example, although Latin Hypercube Sampling is mentioned in the description of the model many times as a key feature, no actual sample design is specified … insufficient details are provided on how or where these numbers are generated, precluding a third party, with suitable software and expertise, from reproducing the results—violating a basic principle of the scientific method.

The NRC report quoted above also lists what needs to be captured in an adequate documentation of a risk analysis (Brisson and Edmunds, 2006 as cited in NRC, 2008):

> It is essential that analysts document the following: (1) how they construct risk assessment models, (2) what assumptions are made to

characterize relationships among variables and parameters and the justifications for these, (3) the mathematical foundations of the analysis, (4) the source of values assigned to parameters for which there are no available data, and (5) the anticipated impact of uncertainty for assumptions and parameters.

TRAM and Risk Analysis and Management for Critical Asset Protection (RAMCAP) are described primarily through manuals that are not widely available; TRAM has never been peer-reviewed. The committee was not provided with any documentation about the risk calculations behind the grants programs—DHS offered that a specific individual could be contacted to answer questions—and likewise has not been given or pointed to detailed documentation of the modeling behind the Maritime Security Risk Analysis Model (MSRAM), CIKR vulnerability analyses, the TSA RMAT model, and so on. The committee has not seen or heard of validation studies of any DHS risk models. These gaps are apparently not due to security concerns, and it is not necessary to publish in the open literature in order to reap the value of documentation and peer review.

Recommendation: DHS should adopt recognized scientific practices for its risk analyses:

- **DHS should create detailed documentation for all of its risk models, including rigorous mathematical formulations, and subject them to technical and scholarly peer review by experts external to DHS.**
- **Documentation should include simple worked-out numerical examples to show how a methodology is applied and how calculations are performed.**
- **DHS should consider a central repository to enable DHS staff and collaborators to access model documentation and data.**
- **DHS should ensure that models undergo verification and validation—or sensitivity analysis at the least. Models that do not meet traditional standards of scientific validation through peer review by experts external to DHS should not be used or accepted by DHS.**
- **DHS should use models whose results are reproducible and easily updated or refreshed.**
- **DHS should continue to work toward a clear, unambiguous risk lexicon.**

The committee recognizes that security concerns at DHS constrain the extent to which some model assumptions and results are made public, but some type of formal review is still required for all elements of models if they are to be used with confidence by the department and others. Such a requirement is consistent with the core criteria for risk analysis as specified in the 2009 NIPP (DHS-IP, 2009).

The Assumptions Embedded in Risk Analyses Must Be Visible to Decision Makers

Of special importance is transparency with respect to decision makers. The assumptions and quality of the data that are provided as inputs and the uncertainties that can be anticipated are essential to establish the credibility of the model. Also of importance are periodic reviews and evaluations of the results that are being obtained using relatively new and old models. These reviews should involve specialists in modeling and in the problems that are being addressed. They should address the structure of the models, the types and certainty of the data that are required (e.g., historical or formally elicited expert judgments), and how the models are intended to be used. The assumptions and quality of the data that are provided as inputs and the uncertainties that can be anticipated are essential to establish the credibility of the model.

Because of the many uncertainties attendant on risk analysis, especially risk analysis related to terrorism, it is crucial that DHS provide transparency for the decision maker. When decision makers must weigh a broad range of risks—including some with very large uncertainties, as in the case of terrorism risk—transparency is even more important because otherwise the decision maker will be hard-pressed to perform the necessary comparison. The analysis needs to communicate the uncertainties to decision makers. In one sense, DHS risk-related processes can be helpful in this regard: in most cases, those who are close to the risk management function will have to be involved in producing vulnerability analyses. This is certainly the case for CIKR sectors, and it is also true for users of TRAM, MSRAM, and probably other risk packages. Conducting a vulnerability analysis requires many hours of focused attention on vulnerabilities and threats, which can also be a very beneficial process for making operations staff more attuned to the risks facing their facilities.

TRAM and some of the models for evaluating infrastructure vulnerabilities are overly complex, which detracts from their transparency. Moreover, it seems that nearly all of DHS's risk models must be run by, or with the help of, a specialist. The only exception mentioned to the committee was a spreadsheet-based model under development by a contractor for the FEMA grants program, which is intended to be used by grant applicants. The ideal risk analysis tool would be one that a risk manager or decision maker can (1) understand conceptually, (2) trust, and (3) get quick turnaround on what-if scenarios and risk mitigation trade-offs. These attributes should be attainable.

Another limitation on transparency is the difficult one posed by classified information. The lack of clearances precludes the possibility of passing on much threat information to DHS's "customers." Even if these customers hold the right clearances, there are also limitations on the availability of secure communications networks and equipment including telephones, faxes, and computers. Vulnerability information is affected by similar constraints. Common sense—and the desire of private sector owners and operators to treat some details as proprietary—dictates that such information should be given limited dis-

tribution.

However, the committee did hear concerns that information about vulnerability from one CIKR sector is not normally shared with those outside that sector, which can limit the insights available to risk managers in sectors (e.g., public health) that are affected by risks to other sectors (e.g., electrical and water supplies).

Recommendation: To maximize transparency of DHS risk analyses for decision makers, DHS should aim to document its risk analyses as clearly as possible and distribute them with as few constraints as possible. As part of this recommendation, DHS should work toward greater sharing of vulnerability and consequence assessments across infrastructure sectors so that related risk analyses are built on common assessments.

References

Abbaspour, K. C., R. Schulin, E. Schlappi, and H. Fluhler. 1996. A Bayesian approach for incorporating uncertainty and data worth in environmental projects. Environmental Modeling and Assessment 1:151-158.

Adams, J., and M. Thompson. 2002. Taking account of societal concerns about risk: Framing the problem. Technical Report RR035, Health and Safety Executive, H. M. Government, London. Available online at *http://www.hse.gov.uk/research/rrpdf/rr035.pdf*. Last accessed December 17, 2009.

Ahuja, R. T., T. Magnanti, and J. Orlin. 1993. Network Flows: Theory, Algorithms, and Applications. Englewood Cliffs, N.J.: Prentice Hall.

Alderson, D. 2008. Catching the network science bug: Insight and opportunity for the operations researcher. Operations Research 56(5):1047-1065.

Alderson, D., G. Brown, and M. Carlyle. 2009. How to assess the value of critical infrastructure: A worst-case view of risk and its implications for defensive investment. November 4. Manuscript submitted for publication. Monterey, Calif.: Naval Postgraduate School, Department of Operations Research.

ASCE (American Society of Civil Engineers) Critical Infrastructure Guidance Task Committee. 2009. Guiding Principles for the Nation's Critical Infrastructure. Washington, D.C. ASME (American Society of Mechanical Engineers) Innovative Technologies Institute. 2008. RAMCAP, Risk Analysis and Management for Critical Asset Protection. Available online at *http://www.asme-iti.org/RAMCAP*. Last accessed November 10, 2009.

Ayyub, B. 2003. Risk Analysis in Engineering and Economics. Ontario, CA: Chapman & Hall, CRC Press.

Bakir, N., and A. Savachkin. 2010. Two countermeasure strategies to mitigate random disruptions in capacitated systems. Journal of Systems Science and Systems Engineering. Available online at *http://www.springerlink.com/content/vn2l1jxxx4097x3u/*. Last accessed April 2, 2010.

Bank for International Settlements. 2006. International Convergence of Capital Measurement and Capital Standards—A Revised Framework Comprehensive Version. Basel: Committee on Banking Supervision. Available online at *http://www.bis.org/publ/bcbs128.pdf*. Last accessed November 30, 2009.

Barker, K., and Y. Y. Haimes. 2009. Assessing uncertainty in extreme events: Applications to risk-based decision making in interdependent infrastructure sectors. Reliability Engineering & System Safety 94(4):819-829.

Barnhart, C. 2009. Irregular operations: Schedule recovery and robustness.

Chapter 4 in P. Belobaba, C. Barnhart, and A. Odoni (eds.), The Global Airline Industry. New York: John Wiley & Sons.

Bazaraa, M., J. Jarvis, and H. Sherali. 2004. Linear Programming and Network Flows. 3rd edition. New York: Wiley-Interscience.

Bedford, T., and R. Cooke. 2001. Probabilistic Risk Analysis: Foundations and Methods. Cambridge, UK: Cambridge University Press.

Bennett, P., and K. Calman. 1999. Risk Communication and Public Health. Oxford, UK: Oxford University Press.

Berry, D. A., and D. K. Stangl (eds). 1996. Bayesian Biostatistics. New York: Marcel Dekker.

Bier, V. M. 2005. Game-theoretic and reliability methods in counter-terrorism and security. Chapter 2 In Modern Statistical and Mathematical Methods in Reliability, Series on Quality, Reliability and Engineering Statistics. Hacksenback, N.J.: World Scientific Publishing Co.

Bier, V. M., and M. Azaiez (eds.). 2009. Game Theoretic Risk Analysis of Security Threats. New York: Springer Science.

Bier, V. M., S. Oliveros, and L. Samuelson. 2007. Choosing what to protect: Strategic defensive allocation against an unknown attacker. Journal of Public Economic Theory 9(4):563-587.

Bier, V., N. Haphuriwat, J. Menoyo, and R. Zimmerman, A. 2008. Optimal resource allocation for defense of targets based on differing measures of attractiveness. Risk Analysis 28(3).

Brand, K. P., and M. J. Small. 1995. Updating uncertainty in an integrated risk assessment: Conceptual framework and methods. Risk Analysis 15(6):719-731.

Brown, G., M. Carlyle, J. Salmeron, and K. Wood. 2005. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. Pp. 102-103 in H. Greenberg and J. Smith (eds.), INFORMS Tutorials in Operations Research: Emerging Theory, Methods and Applications. Hanover, Md.: Institute for Operations Research and the Management Sciences.

Brown, G., M. Carlyle, J. Salmeron, and K. Wood. 2006. Defending critical infrastructure. Interfaces 36(6):530-544.

CDC (Centers for Disease Control and Prevention). 2008. Public Health Preparedness: Mobilizing State by State. Available online at *http://www.bt.cdc.gov/publications/feb08phprep/*. Last accessed January 4, 2010.

Chao, P. T., and B. D. Hobbs. 1997. Decision analysis of shoreline protection under climate change uncertainty. Water Resources Research 33(4):817-830.

Chapman, P., M. Christopher, U. Juttner, H. Peck, and R. Wilding . 2002. Identifying and managing supply chain vulnerability. UK: Cranfield Centre for Logistics and Transportation, Cranfield School of Management.

Clemen, R. T. 1996. Making Hard Decisions: An Introduction to Decision Analysis. 2nd edition. Belmont, Ca.: Duxbury Press.

Committee of the Sponsoring Organizations of the Treadway Commission . 2004. Enterprise Risk Management—Integrated Framework, Executive

Summary.
Cooke, R. M. 1991. Experts in Uncertainty: Opinion and Subjective Probability in Science. New York: Oxford University Press.
Cooke, R. M., and L. H. J. Goossens. 2000. Procedures guide for structured expert judgment in accident consequence modeling. Radiation Protection Dosimetry 90(3):303-309.
Cooke, R. M., A. M. Wilson, J. T. Tuomisto, O. Morales, M. Tainio, and J. S. A. Evans. 2007. Probabilistic characterization of the relationship between fine particulate matter and mortality: Elicitation of European experts. Environmental Science and Technology 41:6598-6605.
Coppersmith, K. J., R. C. Perman, and R. R. Youngs. 2006. Lessons Learned—The Use of Formal Expert Elicitation in Probabilistic Seismic Hazard. Technical Report OSTI ID:893709. Las Vegas, Nev.: Department of Energy, Yucca Mountain Project. Available online at *http://www.osti.gov/bridge/servlets/purl/893709-yw1Tfr/893709.PDF*. Last accessed January 4, 2010.
Cormican, K., D. Morton, and K. Wood. 1998. Stochastic network interdiction. Operations Research 46(2).
Cornell, C. A. 1968. Engineering seismic risk analysis. Bulletin of the Seismological Society of America 58:1583-1606.
Costello, C. J., R. M. Adams, and S. Polasky. 1998. The value of El Nino forecasts in the management of salmon: A stochastic dynamic assessment. American Journal of Agricultural Economics 80:765-777.
Cox, A. 2008. Some limitations of "Risk = Threat × Vulnerability × Consequence" for risk analysis of terrorist attacks. Risk Analysis 28(6):1749-1761.
Cox, A. 2009. Game theory and risk analysis. Risk Analysis 29(7):1062-1068.
Cox, L. A. 2008. What's wrong with risk matrices? Risk Analysis 28(2):497-512.
Cullen, A., and M. J. Small. 2004. Uncertain risks: The role and limits of quantitative analysis. In T. McDaniels and M. Small (eds.), Risk Analysis and Society: An Interdisciplinary Characterization of the Field. Cambridge, UK: Cambridge University Press.
Davidson, J. S., J. W. Fisher, M. I. Hamoons, J. R. Porter, and R. J. Dinan. 2005. Failure mechanisms of polymer-reinforced concrete masonry walls subjected to blast. Journal of Structural Engineering 131(8):1194-1205.
Davies, J. C. (ed.). 1996. Comparing Environmental Risks. Washington, D.C.: Resources for the Future.
DHS (Department of Homeland Security). 2008. National Information Sharing Strategy. Available online at *http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf*. Last accessed December 4, 2009.
DHS. 2009. Homeland Security Grant Program: Program Guidance and Application Kit. Available online at *http://www.fema.gov/government/grant/hsgp/index.shtm*.
DHS-IP (Office of Infrastructure Protection). 2009. National Infrastructure Pro-

tection Plan, Partnering to Enhance Protection and Resiliency. Washington, D.C.: DHS-IP.

DHS-RMA (Risk Management and Analysis). 2009. Terrorism Risk and Natural Hazard Risk: Cross-Domain Risk Comparisons. Updated July 14. Washington, D.C.: DHS-RMA.

DHS-RSC(Risk Steering Committee). 2008. DHS Risk Lexicon. Washington, D.C.: DHS-RSC.

DHS-RSC. 2009. Interim Integrated Risk Management Framework. January. Washington, D.C.: DHS-RSC. FOIA High 2 Exemption applies.

DHS-S&T (Science and Technology Directorate). 2009. Basic Research Focus Areas. May. Washington, D.C.: DHS-S&T.

Dillon, R. L. R. M. Liebe, and T. Bestafka. 2009. Risk-based decision making for terrorism applications. Risk Analysis 29(3):321-335.

Doherty, N. A. 2000. Integrated Risk Management—Techniques and Strategies for Managing Corporate Risk. New York: McGraw-Hill.

Douglas, M. 1987. How Institutions Think. London, UK: Routledge.

Elkins, D., L. Deleris, and M. E. Pate-Cornell. 2004. Analyzing losses from hazard exposure: A conservative probabilistic estimate using supply chain risk simulation. In R. G. Ingalls, M. D. Rossetti, J. S. Smith, and B. A. Peters (eds.), Proceedings of the 2004 Winter Simulation Conference.

Elkins, D., C. LaFleur, E. Foster, J. Tew, B. Bahar, and J. Wilson. 2007. Clinic: Correlated inputs in an automotive paint shop fire risk simulation. In S.G. Henderson, B. Biller, M.-H. Hsieh, J. Shortle, J.D. Tew, and R.R. Barton (eds.), Proceedings of the 2007 Winter Simulation Conference.

EPA (Environmental Protection Agency). 1987. Unfinished Business: A Comparative Assessment of Environmental Problems. EPA 230287025a. Washington, D.C.: EPA.

EPA. 2009. Guidance Document on the Development, Evaluation and Application of Environmental Models. Available online at *http://www.epa.gov/crem/library/cred_guidance_0309.pdf*, pp. 31-32. Last accessed March 2009.

European Commission. 2000. Procedure Guide for Structured Expert Judgment. EUR 18820EN. Nuclear Science and Technology, Directorate-General for Research.

Fennelly, K. P., A. L. Davidow, S. L. Miller, N. Connel, and J. L. Ellner. 2004. Airborne infection with *Bacillus anthracis*—From mills to mail. Emerging Infectious Diseases 10:996-1001.

Finkel, A. M., and J. S. Evans. 1987. Evaluating the benefits of uncertainty reduction in environmental health risk management. Journal Air Pollution Control Association 37:1164-1171.

Finkel, A. M., and D. Golding (eds.). 1995. Worst Things First: The Debate over Risk-Based National Environmental Priorities. Washington, D.C.: Resources for the Future.

Fischhoff, B. 1995. Ranking risks. Risk: Health Safety & Environment 6:189-200.

Fitch, J. P., E. Raber, and D. R. Imbro. 2003. Technology challenges in responding to biological or chemical attacks in the civilian sector. Science 32:1350-1354.

Florig, H. K., M. G. Morgan, K. M. Morgan, K. E. Jenni, B. Fischhoff, P. S. Fischbeck, and M. L. DeKay. 2001. A deliberative method for ranking risks (1): Overview and test bed development. Risk Analysis 21(5):913-921.

Fovino, I. N., M. Masera, and A. De Cian. 2009. Integrating cyber attacks within fault trees. Reliability Engineering & Safety Systems 94(9):1394-1402.

Freeze, R. A., J. W. Massmann, L. Smith, T. Sperling, and B. James. 1990. Hydrogeological decision analysis, 1. A framework. Ground Water 28:738-766.

GAO (Government Accountability Office). 2005. Strategic Budgeting and Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities. GAO-05-824T. Washington, D.C.: GAO.

GAO. 2008. Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-627SP. Washington, D.C.: GAO.

Garrick, B. J., J. E. Hall, M. Kilger, J. C. McDonald, T. O'Toole, P. S. Probst, E.R. Parker, R. Rosenthal, A.W. Trivelpiece, L.A. Van Arsdale, and E.L. Zebroski. 2004. Confronting the risks of terrorism: Making the right decisions. Reliability Engineering and System Safety 86:129-176.

Garthwaite, P. H., J. B. Kadane, and A. O'Hagan. 2005. Statistical methods for eliciting probability distributions. Journal of American Statistical Association 100:680-701.

Golany, B., E. H. Kaplan, A. Marmur, and U. G. Rothblum. 2009. Nature plays with dice—Terrorists do not: Allocating resources to counter strategic vs. probabilistic risk. European Journal of Operational Research 192:198-208.

Golden, B. 1978. A problem in network interdiction. Naval Research Logistics Quarterly 25:711-713.

Greenland, S. 2001. Sensitivity analysis, Monte-Carlo risk analysis, and Bayesian uncertainty assessment. Risk Analysis 21:579-583.

Greenland S. 2006. Bayesian perspectives for epidemiologic research. I. Foundations and basic methods (with Discussion). International Journal of Epidemiology 35:765-778.

Guzzetti, F., C. P. Stark, and P. Salvati. 2005. Evaluation of flood and landslide risk to the population in Italy. Environmental Management 36(1):15-36.

Haimes, Y. 2008. Risk Modeling, Assessment, and Management. 3rd edition. New York: John Wiley and Sons.

Haimes, Y. 2009. On the definition of resilience in systems. Risk Analysis 29(4):498-501.

Haimes, Y., B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian, and K. G. Crowther. 2005. Intraoperability input-output model (IIM) for interdependent sectors: Theory and methodology. ASCE Journal of Infrastructure Systems 11(2):67-79.

Haimes, Y., J. Santos, K. Crowther, M. Henry, C. Lian, and Z. Yan. 2008. Risk analysis in interdependent infrastructures. In E. Goetz and S. Shenoi (eds.),

Critical Infrastructure Protection. New York: Springer.
Hammitt, J. K., and A. I. Shlyakhter. 1999. The expected value of information and the probability of surprise. Risk Analysis 19:135-152.
Heal, G., and H. Kunreuther. 2007. Modeling interdependent risks. Risk Analysis 7(3).
Henderson D. A., T. V. Inglesby, J. G. Bartlett, M. S. Ascher, E. Eitzen, and P. B. Jahrling (Working Group on Civilian Biodefense). 1999. Smallpox as a biological weapon: Medical and public health management. Journal of the American Medical Association 281:2127-2137.
Heinz Center. 2000. The Hidden Costs of Coastal Hazards. Washington, D.C.: Island Press.
Hilton, R. W. 1981. The determinants of information value: Synthesizing some general results. Management Science 27:57-64.
Hora, S. C. 1992. Acquisition of expert judgment: Examples from risk assessment. Journal of Energy Engineering 118(2):136-148.
Iman, R. L., and S. C. Hora. 1989. Bayesian methods for modeling recovery times with an application to the loss of off-site power at nuclear power plants. Risk Analysis 9(1):25-36.
Interagency Performance Task Force on Katrina. 2009. Engineering Risk and Reliability of the Hurricane Protection System. Washington, D.C.: U.S. Army Corps of Engineers.
IOM (Institute of Medicine). 2003. Learning from SARS: Preparing for the Next Disease Outbreak—Workshop Summary. Washington, D.C.: The National Academies Press.
James, B. R., and S. M. Gorelick. 1994. When enough is enough: The worth of monitoring data in aquifer remediation design. Water Resources Research 30(12):3499-3513.
JASON. 2009. Rare Events. Report JSR-09-108. October. McLean, Va.: The MITRE Corporation.
Keeney, R. L., and D. von Winterfeldt. 1991. Eliciting probabilities from experts in complex technical problems. IEEE Transactions on Engineering Management 38(3):191-201.
Kunreuther, H. 2002. Risk analysis and risk management in an uncertain world. Risk Analysis (August).
Kunreuther, H. C., and E. Michel-Kerjan. 2009. At War with the Weather: Managing Large-Scale Risks in a New Era of Catastrophes. New York: MIT Press.
Lindley, T. R., and S. G. Buchberger. 2002. Assessing intrusion susceptibility in distribution systems. Journal of the American Water Works Association 94(6):66-79.
MacDonald, J. A., M. J. Small, and M. G. Morgan. 2008. Explosion probability of unexploded ordnance: Expert beliefs. Risk Analysis 28(4):825-841.
Masse, T., S. O'Neil, and J. Rollins. 2007. The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress. February 2.

Massmann, J., and R. A. Freeze. 1987. Groundwater contamination from waste management: The interaction between risk-based engineering design and regulatory policy, 1. Methodology. Water Resources Research 23:351-367.

McGill, W., B. Ayyub, and M. Kaminsky. 2007. Risk analysis for critical asset protection. Risk Analysis 27(5):1265-1281

Mileti, D. 1999. Disasters by Design. Washington, D.C.: Joseph Henry Press.

Morgan, M. G., and M. Henrion. 1990. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge, UK: Cambridge University Press.

Morgan, M. G., and D. Keith. 1995. Subjective judgments by climate experts. Environmental Science & Technology 29(10):468-476.

Morgan, M. G., B. Fischhoff, L. Lave, and P. Fischbeck. 1996. A proposal for ranking risk within federal agencies. Chapter 6 in J.C. Davies (ed.), Comparing Environmental Risks: Tools for Setting Government Priorities. Washington, D.C.: Resources for the Future.

NRC (National Research Council). 1983. Risk Assessment in the Federal Government: Managing the Process. Washington, D.C.: National Academy Press.

NRC. 1989. Improving Risk Communication. Washington, D.C.: National Academy Press.

NRC. 1994. Science and Judgment in Risk Assessment. Washington, D.C.: National Academy Press.

NRC. 1996. Understanding Risk: Informing Decisions in a Democratic Society. Washington, D.C.: National Academy Press.

NRC. 2002. Making the Nation Safer, the Role of Science and Technology in Countering Terrorism, Chapters 9, 10, and 11. Washington, D.C.: The National Academies Press.,

NRC. 2006. Facing Hazards and Disasters: Understanding Human Dimensions, Washington, D.C.: The National Academies Press.

NRC. 2007a. Elevation Data for Floodplain Mapping. Washington, D.C.: The National Academies Press.

NRC. 2007b. Improving the Nation's Water Security: Opportunities for Research. Washington, D.C.: The National Academies Press.

NRC. 2007c. Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis. Washington, D.C.: The National Academies Press.

NRC. 2007d. Scientific Review of the Proposed Risk Assessment Bulletin from the Office of Management and Budget. Washington, D.C.: The National Academies Press.

NRC. 2007e. U.S.-Russian Collaboration in Combating Radiological Terrorism. Washington, D.C.: The National Academies Press.

NRC. 2008. Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change. Washington, D.C.: The National Academies Press.

NRC. 2009. Mapping the Zone: Improving Flood Map Accuracy. Washington, D.C.: The National Academies Press.

Office of Government Commerce, United Kingdom Cabinet Office. 2002. Management of Risk: Guidance for Practitioners. London, UK: United Kingdom Cabinet Office.

O'Hagan, A., C. Buck, A. Daneshkhah, J. R. Eiser, P. H. Garthwaite, D. J. Jenkinson, J. Oakley, and T. Rakow. 2006. Uncertain Judgments: Eliciting Experts' Probabilities. Chichester, UK: John Wiley & Sons.

Ostfeld, A., J. G. Uber, E. Salomons, J. W. Berry, W. E. Hart, C. A. Phillips, J-P. Watson, G. Dorini, P. Jonkergouw, Z. Kapelan, F. di Pierro, S-T. Khu, D. Savic, D. Eliades, M. Polycarpou , S. R. Ghimire, B. D. Barkdoll, R. Gueli; J. J. Huang, E. A. McBean, W. James; A. Krause, J. Leskovec, S. Isovitsch, J. Xu, C. Guestrin, J. VanBriesen, M. Small, P. Fischbeck, A. Preis, M. Propato, O. Piller, G. B. Trachtman, Z. Y. Wu, and T. Walski. 2008. The Battle of the Water Sensor Networks (BWSN): A design challenge for engineers and algorithms. Journal of Water Resources Planning and Management 134(6):556-568.

Otway, H., and D. von Winterfeldt. 1992. Expert judgment in risk analysis and management: Process, context, and pitfalls. Risk Analysis 12(1):83-93.

Parnell, G. S., C. M. Smith, and F. I. Moxley. 2010. Intelligent adversary risk analysis: A bioterrorism risk management model. Risk Analysis 30(1):32-48.

Paté-Cornell, M. E. 1996. Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety 54:95-111.

Paté-Cornell, M. E., and S. Guikema. 2002. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research 7(4):5-20.

Patwardhan, A., and M. J. Small. 1992. Bayesian methods for model uncertainty analysis with application to future sea level rise. Risk Analysis 4:513-523.

Pidgeon, N., R. Kasperson, and P. Slovic (eds.). 2003. The Social Amplification of Risk. Cambridge, UK: Cambridge University Press.

Raiffa, H. 1968. Decision Analysis: Introductory Lectures on Choice Under Uncertainty, Reading, Mass.: Addison-Wesley.

Rasmussen, N. C. 1976. Probabilistic risk assessment: Its possible use in safeguards problems. Pp. 66-88 in Proceedings of the Institute for Nuclear Materials Management meeting, Fall.

Remennikov, A. M. 2003. A review of methods for predicting bomb blast effects on buildings. Journal of Battlefield Technology 6(3):5-10.

Robert, B., R. De Calan, and L. Morabito. 2008. Modelling interdependencies among critical infrastructures. International Journal of Critical Infrastructures 4(4):392-408.

Savachkin, A. A., N. O. Bakir, and A. Uribe-Sanchez. 2008. An optimal countermeasure policy to mitigate random capacity disruptions in a production system. International Journal of Agile Systems and Manufacturing, Volume 3.

Schneider, P. J., and B. A. Schauer. 2006. HAZUS—Its development and its future. Natural Hazards Review 7(2):40-44.

Settles, G. S. 2006. Fluid mechanics and homeland security. Annual Review of Fluid Mechanics 38:87-110.

Sherali, H. D., J. Desai, and T. S. Glickman. 2008. Optimal allocation of risk-reduction resources in event trees. Management Science 54(7):1313-1321.

Shindo, A., H. Yamazaki, A. Toki, R. Maeshima, I. Koshijima, and T. Umeda. 2000. Approach to potential risk analysis of networked chemical plants. Computers and Chemical Engineering 24(2):721-727.

Slovic, P. 2000. The Perception of Risk. London, UK: Earthscan.

Slovic, P. 2002. Terrorism as hazard: A new species of trouble. Risk Analysis 22:425-426.

Small, M. J. 2004. The value of information for conflict resolution. Pp. 171-194 in I. Linkov and A. Ramadan (eds.), Comparative Risk Assessment and Environmental Decision Making. Dordrecht: Kluwer Academic Publishers.

Smislova, M. 2007. Private Sector Information Sharing: The DHS Perspective and Lessons Learned. Statement of Melissa Smislova, Director, Homeland Infrastructure Threat and Risk Analysis Center, U.S. Department of Homeland Security before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. July 26. Available online at *http://homeland.house.gov/SiteDocuments/20070726123143-15976.pdf*. Last accessed January 7, 2010.

Smith, J. Q., and S. French. 1993. Bayesian updating of atmospheric dispersion models for use after an accidental release of radiation. Statistician 42:501-511.

Smith, J. C., C. Lim, and F. Sudargho. 2007. Survivable network design under optimal and heuristic interdiction scenarios. Journal of Global Optimization 38:181-199.

Sohn, M. D., M. J. Small, and M. Pantazidou. 2000. Reducing uncertainty in groundwater site characterization using Bayes Monte Carlo methods. Journal of Environmental Engineering 126(10):893-902.

Taleb, N. N. 2007. The Black Swan: The Impact of the Highly Improbable. New York: Random House.

Taylor, A. C., J. Evans, and T. McKone. 1993. The value of animal test information in environmental control decisions. Risk Analysis 13:403-412.

TFAH (Trust for America's Health). 2008. Ready or Not? Protecting the Public's Health from Disease, Disaster, and Bioterrorism. Available online at *http://healthyamericans.org/reports/bioterror08/*. Last accessed January 4, 2010.

Thompson, M., R. Ellis, and A. Wildavsky. 1990. Cultural Theory. Boulder, Colo.: Westview Press.

Turner, B.A., and N.F. Pidgeon. 1997. Man-made Disasters. Oxford, UK: Butterworth-Heineman.

Toner, E., R. Waldhorn, C. Franco, B. Courtney, A. Norwood, K. Rambhia, T. Inglesby, and T. O'Toole. 2009. Hospitals Rising to the Challenge: The First Five Years of the U.S. Hospital Preparedness Program and Priorities Going Forward. Available online at *http://www.upmc-biosecurity.org/web-*

site/resources/publications/2009/2009-04-16-hppreport.html. Last accessed January 4, 2010.

UK Treasury. 2004. The Orange Book: Management of Risk - Principles and Concepts. London, UK: Treasury.

Verweij, M. (ed.). 2006. Clumsy Solutions for a Complex World: Governance, Politics, and Plural Perceptions. Global Issues Series. New York: Palgrave Macmillan.

von Winterfeldt, D., and T. M. O'Sullivan. 2006. Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? Decision Analysis 3(2):63-75.

Wagner, B. J. 1995. Sampling design methods for groundwater modeling under uncertainty. Water Resources Research 31(10):2581-2591.

Wagner, B. J. 1999. Evaluating data worth for ground-water management under uncertainty. Journal of Water Resources Planning & Management 125(5):281-288.

Wang, L., and Q. Chen. 2008. Applications of a coupled multizone and CFD model to calculate airflow and contaminant dispersion in built environment for emergency management. HVAC&R Research 14(6):925-939.

Walton, J. 2008. Scanning beyond the horizon: Exploring the ontological and epistemological basis for scenario planning. Advances in Developing Human Resources 10(2):147-165.

Willis, H. H. 2007. Guiding resource allocations based on terrorism risk. Risk Analysis 27(3):597-606.

Willis, H. H., M. L. DeKay, M. G. Morgan, H. K. Florig, and P. S. Fischbeck. 2004. Ecological risk ranking: Development and evaluation of a method for improving public participation in environmental decision making. Risk Analysis 24:363-378.

Willis, H. H., A. R. Morral, T. K. Kelly, and J. Medby. 2005. Estimating Terrorism Risk. MG-388-RC. Santa Monica, Ca.: RAND Corporation.

Winkler, R. L., and A. H. Murphy. 1985. Decision analysis. Pp. 493-524 in A. H Murphy and R. W. Katz (eds.), Probability, Statistics, and Decision Making in the Atmospheric Sciences. Boulder, Co.: Westview Press.

Wolfson, L. J., J. B. Kadane, and M. J. Small. 1996. Bayesian environmental policy decisions: Two case studies. Ecological Applications 6(4):1056-1066.

Yu, G., and X. Qi. 2004. Disruption management: Framework, Models and Applications. Link, Singapore: World Scientific.

Zhuang, J., and V. M. Bier. 2007. Balancing terrorism and natural disasters—Defensive strategy with endogenous attacker effort. Operations Research 55(5):976-991.

Zickfield, K., A. Levermann, M. G. Morgan, T. Kuhlbrodt, S. Rahmstorf, and D. W. Keith. 2007. Expert judgments on the response of the Atlantic meridional overturning circulation to climate change. Climatic Change 82:3-265.

Appendixes

Appendix A
Characterization of Uncertainty[1]

The characterization of uncertainty is recognized as a critical component of any risk assessment activity (Cullen and Small, 2004; NRC, 1983, 1994, 1996, 2008). Uncertainty is always present in our ability to predict what might occur in the future, and is present as well in our ability to reconstruct and understand what has happened in the past. This uncertainty arises from missing or incomplete observations and data; imperfect understanding of the physical and behavioral processes that determine the response of natural and built environments and the people within them; and our inability to synthesize data and knowledge into working models able to provide predictions where and when we need them.

A key element of effective treatments of uncertainty is the ability to clearly distinguish between the (inherent) variability of a system, often referred to *aleatory* or *statistical uncertainty*, and the (reducible) uncertainty due to lack of full knowledge about the system, referred to as *epistemic* or *systematic uncertainty*. The former applies to processes that vary randomly with time, or space, or from sample to sample (e.g., person to person, item to item). Even if a perfectly specified probability model is available to describe this variation, the inherent variability dictates that we are uncertain about what will occur during the next year or decade, at the next location, or for the next sample.

Models that consider only variability are typically formulated for well-characterized, well-understood systems such as those assumed to follow the rules of probability (flipping coins, tossing dice, choosing cards from a deck) or those for which a long period of observation has given us confidence that the probabilities are estimated with a high degree of precision, such as weather outcomes, common accident rates, or failure probabilities for manufactured parts that have been tested and used by the tens of thousands or more. Even in these cases, however, unrecognized nonstationarity (changes that occur over time)—for example, from climate change—can render historical estimates inaccurate and uncertain for future prediction. In these cases, uncertainty in our characterization of variability must also be considered.

To illustrate the combined effects of variability and uncertainty on future predictions, consider an event that has known probability of occurrence in a year of p^*. Consider the simple case where a single event occurs during each year with probability p^*, or no event occurs (with probability $1 - p^*$). The probability

[1] References for this appendix A are included in the report's "References."

distribution function for the number of events that might occur in the next N years is given by the well-known binomial distribution, with expected value p^*N, but with some chance for more than this number of events occurring during the next N years, and some chance of less. For example, if $p^* = 0.15$ (a 15 percent chance of an event occurring each year) and $N = 20$ years, the expected number of events over the 20-year period is $0.15 \times 20 = 3$ events. We can also calculate the standard deviation for this amount ($= [p^*(1- p^*)N]^{1/2}$), which in this case is calculated to be 1.6 events. All this, however, assumes that we are certain that $p^* = 0.15$. In most homeland security modeling, such certainty will not be possible because the assumptions here do not hold for terrorism events. A more sophisticated analysis is needed to show the implications of our uncertainty in p^* in those cases.

A common model used to represent uncertainty in an event occurrence probability, p (e.g., a failure rate for a machine part), is the beta distribution. The beta distribution is characterized by two parameters that are directly related to the mean and standard deviation of the distribution of p; this distribution represents the uncertainty in p (i.e., the true value of p might be p^*, but it might lower than p^* or higher than p^*). The event outcomes are then said to follow a beta-binomial model, where the "beta" part refers to the uncertainty and the "binomial" part refers to the variability. When the mean value of the beta distribution for p is equal to p^*, the mean number of events in N years is the same as that calculated above for the simple binomial equation (with known $p = p^*$). In our example, with mean $p = p^* = 0.15$ and $N = 20$ years, the expected number of events in the 20-year period is still equal to 3. However, the standard deviation is larger. So, for example, if our uncertainty in p is characterized by a beta distribution with mean = 0.15 and standard deviation = 0.10 (a standard deviation nearly as great or greater than the mean is not uncommon for highly uncertain events such as those considered in homeland security applications), then the standard deviation of the number of events that could occur in the 20-year period is computed to be 2.5. This is 60 percent larger than the value computed above for the binomial case where p is assumed known (standard deviation of number of events in 20 years = 1.6), demonstrating the added uncertainty in future outcomes that can result from uncertainty in event probabilities. This added uncertainty is also illustrated in Figure A-1, comparing the assumed probability distribution functions for the uncertain p (top graph in Figure A-1) and the resulting probability distribution functions for the uncertain number of events occurring in a 20-year period (bottom graph in Figure A-1) for the simple binomial and the beta-binomial models. As indicated, the beta-binomial model results in a greater chance of 0 or 1 event occurring in 20 years, but also a greater chance of 7 or more events occurring, with significant probability up to and including 11 events. In this case, characterizing the uncertainty in the threat estimate is clearly critical when estimating the full uncertainty in future outcomes.

Proper recognition and characterization of both variability and uncertainty is important in all elements of a risk assessment, including effective interpreta-

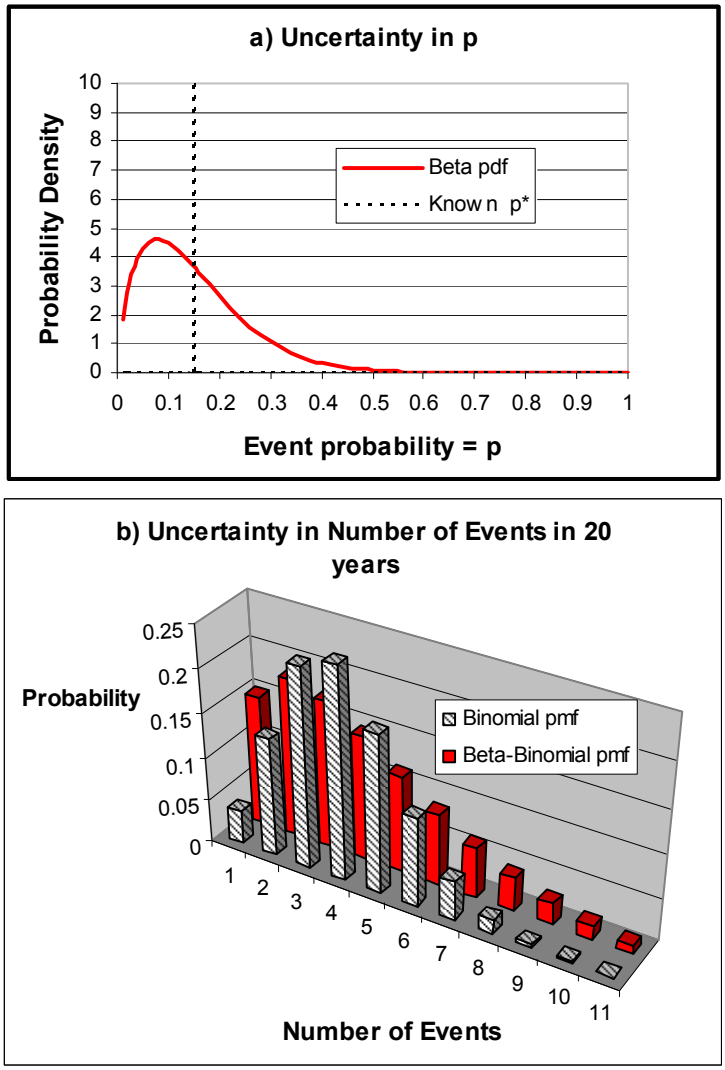

FIGURE A-1 Comparison of binomial model assuming known event probability *p* and beta-binomial model assuming that event probability is uncertain:(a) uncertainty distribution for *p*; mean of uncertain beta distribution is equal to the known value *p** for the binomial case;((b) distribution of number of events in a future 20-year period; the binomial distribution considers only variability while the beta-binomial model reflects both variability and uncertainty.

tion of vulnerability, consequence, intelligence, and event occurrence data as they are collected over time. It also provides a basis for identifying which data are most critical to collect to reduce the uncertainties that matter for decision making, using a value-of-information approach as described below.

A range of analytical and numerical methods are available to estimate the uncertainty in model predictions resulting from uncertain model structure and inputs. A key objective in applying these methods is to evaluate which assumptions and inputs are most important in determining model output (through sensitivity analysis) and model uncertainty (through uncertainty analysis), especially those uncertainties that matter for (1) consistency with observed data and (2) the response and management decisions that are informed by the model. Studies to reduce the uncertainty in these assumptions and inputs then become prime targets in the value-of-information approach described below. Bayesian methods are especially useful for integrating new information as it becomes available, allowing iterative recalibration of model parameters and output uncertainty over time.

Learning and the Value of Information

A key element of risk-based management for homeland security and natural disasters is deciding which additional information collection efforts would be most beneficial to provide the key knowledge for more effective decisions. Effort invested in intelligence gathering is intrinsically viewed from this perspective; investments in more routine data collection and long-term research should be viewed similarly. When risk assessments include an explicit representation of uncertainty, the value of new information can be measured by its ability to reduce the uncertainties that matter in subsequent decisions derived from the risk analyses. A number of methods have been developed to quantify this, including scientific estimates based on variance reduction, decision-analytic methods based on the expected value of decisions made with and without the information, and a newer approach based on the potential for information to yield consensus among different stakeholders or decision makers involved in a risk management decision. These approaches are briefly reviewed.

Scientists and engineers often focus on the uncertainty variance of predicted outcomes from their assessments and how much this variance might be reduced by new or additional data (e.g., Abbaspour et al., 1996; Brand and Small, 1995; Chao and Hobbs, 1997; James and Gorelick, 1994; Patwardhan and Small, 1992; Smith and French, 1993; Sohn et al., 2000; Wagner, 1995, 1999). Although determining the uncertainty variance of model predictions and the potential to reduce them is very useful, this is in principle just the first step in characterizing the value of information. The key question is: In the context of pending risk management decisions, do the uncertainties matter? To address this question, the decision sciences have developed a decision analytic framework for the value of information (VOI) that considers: (1) whether the reduced uncertainty

could lead the decision maker to alter their decision and (2) what the expected increase in monetary value of the decision is as a result of the new information.

Decision analysis provides formal methods for choosing among alternatives under uncertainty, including options for collecting more information to reduce the uncertainty so that the outcomes associated with the alternatives are predicted with greater accuracy and precision (Chao and Hobbs, 1997; Clemen, 1996; Keeney, 1982; Raiffa, 1968; Winkler and Murphy, 1985). With no options for further study or data collection, the rational, fully informed decision maker will choose the option that maximizes the expected utility (or equivalently, minimizes the expected reduction in utility). Other decision rules may be considered as well, such as minimizing the maximum possible loss for a risk-averse decision maker.

When a possible program for further study or data collection is available, it should be chosen only if its results have the potential to influence the decision maker to change his or her preferred pre-information (prior) decision, and only if the increase in the expected value of the decision exceeds the program's cost. Since information of different types and different quality can be considered, and these can affect the uncertainty of in the predicted outcomes associated with alternative decisions in different ways, a number of different measures of VOI can be considered (Hammitt and Shlyakhter, 1999; Hilton, 1981; Morgan and Henrion, 1990), including the following:

1. The Expected Value of Perfect Information (EVPI): how much higher is the expected value of the optimal decision when all uncertainty is removed?
2. The Expected Value of Perfect Information About X (EVPIX): how much higher is the expected value of the optimal decision when all of the uncertainty about a particular aspect of the problem, X (e.g., a particular input to an infrastructure simulation model), is removed?
3. The Expected Value of Sample Information (EVSI): how much higher is the expected value of the optimal decision made contingent upon the results of a sampling or research program that has less than perfect information, that is, with finite sample size and/or the presence of some measurement error?

Examples demonstrating the computation of these different measures of VOI have been developed for environmental decisions (Abbaspour, 1996; Freeze et al., 1990; James and Gorelick, 1994; Massmann and Freeze, 1987a,b; Wagner, 1999) and other elements of an integrated risk or economic assessment (Costello et al., 1998**;** Finkel and Evans, 1987; Taylor et al., 1993).

The basic decision-analytic approach described above assumes a single decision maker with a single set of valuations for the outcomes, a single set of prior probabilities for these outcomes under the different decision options, and a fixed and known mechanism for translating study results into posterior probabilities (i.e., a known and agreed-upon likelihood function for the proposed or ongoing research and data collection). However, for many decisions, multiple stakeholders with different values and beliefs must deliberate and come to some

consensus, informed by the science and the study results, but also affected by their differing valuations, prior probabilities and interpretation, and trust in scientific studies. This often leads to conflict in the decision process or, when one party has the authority or power to impose its will on others, dissatisfaction of the other parties with the decision outcome. What is needed then is a decision-analysis framework that identifies the sources of these differences and provides a rational basis for concrete steps that can overcome them. This leads to a broader and potentially more powerful notion of information value, based on the value of information for conflict resolution.

The idea that better information could help to facilitate conflict resolution is an intuitive one. If part of the failure to reach consensus is due to a different view of the science—a disagreement over the "facts"—then a reduction in the uncertainty concerning these facts should help to eliminate this source of conflict. Scientists often disagree on the facts (Cooke, 1991; Hammitt and Shlyakhter, 1999; Morgan and Keith, 1995). While the source of this disagreement may stem from ("legitimate") disciplinary or systematic differences in culture, perspective, knowledge, and experience or ("less legitimate," but just as real) motivational biases associated with research sponsorship and expectation, strong evidence that is collected, peer-reviewed, published, tested and replicated in the open scientific community and literature should lead eventually to a convergence of opinion. The Bayesian framework provides a good model for this process: even very different prior distributions should converge to the same posterior distribution when updated by a very large sample size with accurate and precise data.

Consider now a decision-analytic framework that must translate the implications of changes in assessments resulting from new information for scientists and the "decision support community" into new assessments for decision makers and interested and affected parties. Even were the science to be perfect and all scientists and stakeholders agree that the outcomes associated with each decision option are known with certainty, the different stakeholders to the problem are likely to value these outcomes differently, due to real or perceived differences in allocation of the benefits, costs, and risks associated with them. Measures of VOI for this situation must thus consider the likelihood that the information will convince conflicting participants to reach consensus, a situation of relevance to Department of Homeland Security (DHS). A VOI for conflict resolution has been proposed for this purpose (Small, 2004), and (Adams and Thompson, 2002; Douglas, 1987; Thompson et al., 1990; Verweij, 2006) addresses the underlying problem of policy analysis where stakeholder groups have very diverse worldviews. These differing ways of evaluating the VOI in a risk analysis should be considered by DHS in developing its research and data collections programs.

Appendix B
Evolution of Risk Analysis at EPA

In examining the quality and utility of Department of Homeland Security (DHS) approaches to risk assessment, the committee decided there would be value in reviewing the practices of other federal agencies that have invested heavily in risk assessment and that now have relatively mature programs. The Environmental Protection Agency (EPA) has a substantial record of performance in this area, but similar activities at agencies such as the Occupational Safety and Health Administration (OSHA), the Food and Drug Administration (FDA), and the Department of Health and Human Services (DHHS) Agency for Toxic Substances and Disease Registry (ATSDR) are also informative.[1] In fact, the risk assessment activities of these agencies have much in common, and all draw heavily from a long series of expert reports on risk assessment from the National Academies and other bodies. This appendix contains a brief summary of the essential features of the relatively well established approaches to risk assessment at the EPA, and it also provides a look at how the decision needs of the EPA are satisfied by the approaches taken. Information for this appendix derives from a number of EPA guidelines and policy statements, citations to some of the relevant documents of other federal agencies, and reports of the National Academies, most especially the report released in December 2008 called *Science and Decisions: Advancing Risk Assessment*. That latter report contains exhaustive documentation of the evolution of these advisory reports and of their implementation over the past 25 years.

This appendix also examines how some of the principles upon which EPA risk assessment approaches are based might be applicable to DHS.

HISTORICAL BACKGROUND

Over a period of several decades, from the 1930s through the 1970s, federal public health and regulatory agencies were given legal authorities to develop scientific information on various agents—chemical, biological, radiological—whose presence in the environment (the workplace, air, water, food, soils, and consumer products) could threaten human health and, further, to take action to limit or eliminate human exposures when health threats were found to be significant. In a few cases, laws require that manufacturers wishing to introduce

[1] There are, of course, risk assessment programs at many other agencies, directed at many different sources of risks to health and safety.

certain substances (food additives, pesticides, pharmaceuticals) develop the information needed to evaluate health threats, and they are further required to gain regulatory approvals to market their products. Products requiring premarket approval can be barred from commerce if regulators determine that their safety is questionable. In most cases, however, the agencies are required to develop health-related information, or to use information published in the scientific literature, to assess threats to health and to establish whether the threat is sufficient to support actions to reduce it. This latter model closely approximates the situation at DHS.

Until the mid- to late 1970s, agency approaches to what later came to be called risk analysis were not highly explicit, and they involved no clearly identified and scientifically justified methodology (NRC, 1983). Indeed, scientific and policy controversies of several kinds rose to the surface in the late 1970s and gave rise to much public concern over the use of scientific information by federal agencies. These concerns prompted a congressionally mandated review by the National Academies, resulting in a report entitled *Risk Assessment in the Federal Government: Managing the Process* issued by the National Research Council in 1983. That report, which is commonly known as "the Red Book," contained a review and analysis of the scientific and policy controversies that had given rise to it (including allegations that federal risk assessments were often "manipulated" to yield the results desired by decision makers), and it offered a way forward that laid a foundation for risk analysis that continues to this day. Many critics of the 1983 report have focused on the awkwardness of the way it portrayed the relationships of analysis to decision making, and this problem has been corrected in the recent *Science and Decisions* report (NRC, 2008b). However, the principles for risk analysis set forth in the 1983 report remain in place, and they have been relied upon by the EPA and other federal agencies. The structure of the risk analysis process and definitions of key terms first handed down in the 1983 report remain in place.

Among the several key principles elaborated in the 1983 report, and affirmed in every expert report that has followed, is the need for care in making inferences beyond what has been shown rigorously. Risk-related information collected through various types of scientific investigations (observational and experimental studies) can reveal risks that directly apply only under limited conditions, and the use of such information to assess risks under different conditions requires the imposition of inferences from (or extrapolation beyond) the data. Two examples help to illustrate this problem:

1. Studies in certain occupational settings in which workers were exposed to high levels of benzene have consistently provided an association between those exposures and excess risks of leukemia. The EPA and other agencies seek to understand whether benzene exposures experienced by the general population, exposures that are typically several orders of magnitude lower than those observed in the workplace, might also pose a risk of leukemia. OSHA is similarly concerned to understand whether the current occupational exposures, again

lower than those found to be associated with excess rates of leukemia, are a health threat. It is nearly impossible to collect risk information for the general population, and it is difficult to collect current occupational exposures because the tools of epidemiology are currently inadequate to these tasks. EPA and OSHA must nevertheless reach some conclusion about general and occupational population risks and then act on that conclusion if risks are found to be excessive.

2. Studies in experimental animals, usually performed at exposure levels in great excess of human exposures, must be relied on in many circumstances, because human (epidemiology) data either are not available or are insufficient to assess causation.

As the 1983 NRC report noted, the EPA (and other agencies) must either adopt some "inference options" for assessing risks under circumstances different from those under which direct risk information is (or can be) collected and measured, or else conclude that nothing at all can be said about the (unmeasured or unmeasurable) risk. The latter conclusion is not a real option because the EPA and its sister agencies could not then fulfill their legal mandate, which is protection of human health.

Of course, some scientific evidence is required to make the inference that health risks can exist under exposure conditions different from those at which they can be measured directly and also to support the case that data developed in experimental animals are useful for evaluating risks to humans. The problem is the lack of scientific evidence and understanding sufficient to determine with accuracy the nature of the inferences that should be used. Indeed, in many cases it is not even possible to determine how inaccurate any given inference might be.

The 1983 NRC report recommended the development by agencies of specific and generally applicable inference options for each of the many types of inferences required to move from limited data to the assessment of health risks. It was recognized that some scientific support could be found for each of the important inferences (or extrapolations), but that the incompleteness of scientific knowledge limited that support. Moreover, in some cases, several inference options might be available and have similarly incomplete scientific bases.

The NRC (1983) report, faced with these conclusions, urged the agencies to develop *general guidelines* for the conduct of risk assessments. These guidelines would include the scientific basis for risk assessments and would also include the specific inference options that would generically be applied in the conduct of those assessments. It was recognized that the selection of specific inferences from among the options available would involve both scientific and policy choices (the latter different in kind from the policy choices involved in risk management), but that as long as the bases for the choices were made explicit, the agencies would be on solid ground: their assessments would at least be consistent, if not scientifically accurate, and would not easily be manipulated (by, for example, selecting on a case-by-case basis the inference options that yielded

the decision makers' preferred result).

The 1983 committee and many subsequent committees, including the one that produced *Science and Decisions* (NRC, 2008b), also recognized that in specific cases (e.g., evaluating the risks associated with a specific chemical) scientific studies might provide evidence that one or more of the generic inferences used by the agencies could be inappropriate. In such circumstances, the agency was encouraged to move from the generic inference to the scientific data available on that specific chemical.

These issues of inference options and policy choices within the risk assessment process might have some applicability to the way DHS approaches its mandate for risk assessment (see below).

EPA PRACTICES

The EPA has developed, and periodically revised, extensive guidelines for the conduct of risk analysis, and over the past three decades it has conducted thousands of risk analyses based on them. The agency has also issued regulations of many types based on these risk analyses. It is well acknowledged that all of these risk analyses contain scientific uncertainties (which vary according to the nature of the data upon which the analyses are based and the number and types of inferences beyond the data that must be made), but they are nevertheless used to support decisions. Although management approaches vary among the different categories of regulated exposures, all regulations are designed to ensure human health protection, by ensuring an adequate degree of risk control.

Most EPA risk analyses focus on chemical contaminants of air, food, water, and soils, but some also include microbial pathogens and radiation-emitting agents. In some cases (e.g., those relating to pesticides or certain industrial chemicals), EPA analyses are directed at commercial products to which people might become exposed. The approach to risk analysis for all of the classes of agents and exposure media is the same, and it is based on the guidelines described earlier. Yet, although risk-analysis methodologies are consistent across different classes of agents, the data upon which these analyses are based can vary greatly among them. Further discussion of this issue is useful, because it may assist understanding of the types of problems DHS encounters in dealing with both risk information that has relatively strong support (natural hazards data) and the far-less-certain information pertaining to terrorist threats.

Thus, EPA's analyses of health risks associated with the so-called primary air pollutants (nitrogen and sulfur oxides, ozone, lead, particulate matter) are based on large bodies of epidemiological data, providing relatively direct measures of human morbidity and mortality. Risk analyses based on such data require the imposition of relatively few inferences beyond the data. Many other analyses conducted by the agency are based on far less certain data (e.g., data drawn entirely from studies in experimental animals) and cannot be completed without the use of a relatively large number of inferences beyond the data. Analogies can

be drawn between these two examples of EPA risk analyses and natural hazards risk analysis, on the one hand, and terrorist-related risk analysis on the other. It is perhaps possible to draw from the EPA experience to assist DHS in its stated goals of combining natural hazards and terrorist-related risks within a single methodological framework (see below).

One other aspect of EPA risk analyses needs to be noted. These analyses provide estimates of *absolute risk*: that is, they are designed to characterize the probabilities of different types of harm associated with exposures to hazardous agents. Risk management decisions seek to reduce risks in accordance with specified, absolute risk criteria for human health protection. Many of the risk analyses thus far conducted by DHS involve *risk ranking*, based on scales of presumed relative risks, and do not include attempts to provide absolute measures of risk. Thus, faced with two major sources of risk—those from natural hazards and those related to terrorist activities—DHS has thus far chosen to examine each source separately and not to compare the absolute risks from the two sources.

RISK ASSESSMENT AND DECISIONS

The 2008 NRC report *Science and Decisions* placed heavy emphasis on the need to ensure that risk analyses[2] are undertaken only when the decisions they are intended to support (or the problems they are intended to deal with) have been well defined and understood by both decision makers and risk analysts. The committee that authored the 2008 report found that, although it is commonly assumed that one must understand how a risk analysis will be used and what decisions it is meant to impact, those questions are not always addressed by agencies prior to conducting the risk analysis, or they may be approached in a less than systematic or complete way.

Risk analyses can be undertaken at many different levels of complexity and completeness and with varying degrees of care regarding uncertainties. Only by ensuring that the analysis is firmly linked in advance to the specific problem that it is intended to evaluate can the utility of the analysis for ultimate decision making be ensured. "Utility" was regarded in the 2008 report as a critical and highly desirable attribute of risk analyses.

The EPA and other agencies were found by the 2008 study to have made significant progress toward incorporating a "Scoping and Problem Formulation" phrase into their practices, to evaluate the purpose of a risk analysis prior to undertaking it. The report strongly urged continuing efforts in this area. It is also clear that this early phase is useful for ensuring that the specific problem to be dealt with is completely delineated and understood by all stakeholders. These important recommendations are applicable in all decision making contexts involving the use of technical information and analysis and certainly include those

[2] The same emphasis is given to any other technical analyses needed to support decisions.

that are within the mandate of DHS.

EPA'S DEVELOPMENT OF RESOURCES TO SUPPORT RISK ANALYSIS AND MANAGEMENT

The EPA, over the past three decades, has devoted much effort to building a capacity for risk analysis that is directed at supporting the decision needs of its various regulatory programs. The model for this development has been based on the concept, first elaborated in the 1983 NRC report, that information arising from research and other sources is not useful without evaluation and synthesis, the latter describing the risk analysis process. Thus, an internal staff, comprised of all the necessary scientific disciplines, is now available to conduct risk analyses on behalf of the agency's decision makers. The staff is augmented by some degree of contractor support, but the agency has found that a strong internal risk analysis capacity is essential. The internal staff not only conducts risk analyses, but also develops and maintains risk analysis guidelines. As noted, these guidelines are essential to ensuring the scientific status and consistency of agency assessments. Internal EPA experts are devoted to conducting analyses (following guidelines) and are also involved in the development of new methods for such analyses.

The research efforts of the EPA are intended to provide the data and knowledge necessary for the development of needed risk analyses. As many reports from the National Academies, including the seminal 1983 report, have emphasized, the conduct of risk analyses reveals clearly the gaps in knowledge and data that need to be filled by research. Risk analysis is thus not only a guide to decisions, but also a sound guide to research. The EPA has adopted this concept, and it would seem to be generally applicable to any institutional context in which a research and data development effort is required to support risk analysis. As with any similar efforts undertaken by large, complex institutions, implementation of such risk-based research programs is bound to be imperfect, but it can be strengthened if an internal staff, focused on the conduct and uses of risk analysis, is firmly entrenched in the life of the agency.

Finally, the use of scientific peer review has become critical to ensuring the quality and utility of EPA risk analyses. Scientific peer review and advisory panels are firmly embedded at several different levels within the EPA.

Appendix C
List of Committee Meetings and Site Visits

November 24-25, 2008, Washington, D.C.: First full committee meeting

February 4-5, 2009, Washington, D.C.: Second full committee meeting

March 19, 2009, Environmental Protection Agency (EPA) Headquarters, Washington, D.C.: Subgroup meeting with EPA to learn about how the agency collaborates with the Department of Homeland Security (DHS) in developing risk assessments

March 2009, Cincinnati, Oh.: committee member meeting with EPA Office of Research and Development (ORD) National Homeland Security Research Center (NHSRC) to learn how DHS activities in risk assessment inform and benefit the efforts of the EPA to advance risk assessment and management tools in its areas of focus

April 8, 2009, Jersey City, N.J.: Subgroup site visit to Port Authority of New York and New Jersey to learn about collaboration with DHS in developing the Transportation Risk Analysis Method (TRAM) risk analysis tool

May 6, 2009, Washington, D.C.: Subgroup site visit to Department of Health and Human Services to discuss collaboration with DHS

May 21-22, 2009, Washington, D.C.: Third full committee meeting

June 3, 2009, Washington, D.C.: Subgroup meeting with DHS Office of Infrastructure Protection (IP) staff to learn about IP programs and activities of the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

July 8, 2009, Washington, D.C.: Subgroup meeting with the Federal Emergency Management Agency (FEMA) to discuss Homeland Security Grants Program and the Cost-to-Capability Initiative

July 8-9, 2009, Clarendon, Va.: Committee member attendance at the Third Annual Fusion Center and Information Sharing Strategy Conference

July 13, 2009, Raleigh, N.C.: Subgroup site visit with the North Carolina Division of Emergency Management to discuss its partnership with DHS in achieving homeland security goals in the state

July 20, 2009, Monterey, Ca.: Subgroup visit to Naval Postgraduate School (NPS) to learn about how NPS advises the Navy and the Department of Defense on risk analysis, particularly vulnerability analyses and consequence analyses

August 17, 2009, Albuquerque, N.M.: Subgroup visit to National Infrastructure Simulation and Analysis Center (NISAC) to learn how the center supports DHS risk-based decision making

August 24-25, 2009, Irvine, Ca.: Fourth full committee meeting

October 16, 2009, Washington, D.C.: Meeting with DHS staff from RMA, the Science and Technology Directorate, Office of the Chief Financial Officer, and the Domestic Nuclear Detection Office

October 21, 2009, Washington, D.C.: Final full committee meeting

Appendix D
Presenters and Resource Persons at the Committee's Information-Gathering Meetings

David Alderson, Naval Postgraduate School (NPS)
Ross Ashley, DHS, FEMA
Sid Baccam, Department of Health and Human Services (DHHS)
Louis Barani, Port Authority of New York and New Jersey (PANYNJ)
Patrick Beggs, DHS, NPPD-CS&C
Michael Beland, Staff, House of Representatives Committee on Homeland Security
Steve Bennett, DHS, NPPD-RMA
Jerry Brashear, American Society of Mechanical Engineers (ASME)
Scott Breor, DHS, RMA
Tommy Brown, DHS, NPPD-IP
Ernesto Butcher, PANYNJ
Matthew Carlyle, NPS
Rocco Casagrande, DHHS
Steve Chase, DHS, I&A
Tony Cheesebrough, Government Accountability Office (GAO), later DHS, NPPD-RMA
Susan Cibulsky, DHHS
Amy Culbertson, DHS, PA&E
Matthew Clark, DHS, S&T
Dan Cooler, DHS, I&A
Dave Cooper, DHS, USCG
Andrew Cox, DHS, TSA
Mike Daniska, North Carolina Emergency Management (NCEM)
Mike DePallo, PANYNJ
John Dorfman, NCEM
Jeff Fuller, Teledyne Brown Engineering
Tina Gabbrielli, DHS, NPPD-RMA
Mark Harvey, DHS, NPPD-FPS
Mike Hevey, Battelle
Mary Beth Hill-Harmon, DHHS
H. Douglas Hoell, Jr, NCEM
Jim Holm, Staff, House of Representatives Committee on Appropriations
Michael Jawer, ASME
Ed Jenkins, NCEM
Linda Kanz, DHS, NPPD-IP

Jin Kim, DHS, NPPD-IP
Jeffrey Kline, NPS
Robert Kolasky, DHS, NPPD-RMA
RADM Arthur Lawrence, DHHS
Micah McCutchan, ABS Consulting
Matthew McKean, DHS, TSA
Mike Molino, SAIC
Matt Mowrer, ABS Consulting
Nitin Natarajan, DHHS
Mike Norman, DHS, NPPD-IP
John Paczkowski, PANYNJ
Don Parente, PANYNJ
Cayce Parrish, U.S. Environmental Protection Agency (EPA)
Dan Pless, Sandia National Laboratories
Kristine Poptanich, DHS, NPPD-IP
Sharla Rausch, DHS, S&T
Juan Reyes, EPA
Steven Sloan, NCEM
Steven Streetman, contractor to DHS, DNDO
Chel Stromgren, SAIC support to DHS
Tracey Trautman, DHS, FEMA
Brandon Wales, DHS, NPPD-IP
Alan Washburn, NPS
Elaine Wethen, NCEM
John Whitley, DHS, PA&E
Roy Wright, DHS, FEMA
John Yarboro, NCEM
Shalanda Young, Staff, House Committee on Appropriations

Appendix E
Committee Biographical Information

John F. Ahearne (NAE), *chair*, is executive director emeritus of Sigma Xi, the Scientific Research Society; emeritus director of the Sigma Xi Ethics Program; and an adjunct professor of engineering at Duke University. Prior to working at Sigma Xi, Dr. Ahearne served as vice president and senior fellow at Resources for the Future and as commissioner and chair of the U.S. Nuclear Regulatory Commission. He worked in the White House Energy Office and as deputy assistant secretary of energy. He also worked on weapons systems analysis, force structure, and personnel policy as deputy and principal deputy assistant secretary of defense. Serving in the U.S. Air Force (USAF), he worked on nuclear weapons effects and taught at the USAF Academy. Dr. Ahearne's research interests include risk analysis, risk communication, energy analysis, reactor safety, radioactive waste, nuclear weapons, materials disposition, science policy, and environmental management. He was elected to the National Academy of Engineering in 1996 for his leadership in energy policy and the safety and regulation of nuclear power. Dr. Ahearne has served on numerous National Research Council (NRC) Committees, having chaired several, and is a former president of the Society for Risk Analysis. Dr. Ahearne earned his Ph.D. in physics from Princeton University in 1966.

Gregory B. Baecher (NAE) is the G.L. Martin Professor of Engineering in the Department of Civil and Environmental Engineering at the University of Maryland, College Park. His primary area of expertise is in infrastructure assessment and protection, with particular concern to waterways. His research also focuses on geoenvironmental engineering, reliability and risk analysis, and environmental history. Dr. Baecher has much NRC experience: he is a past member of the Water Science and Technology Board and the Board on Earth Sciences and Resources and has served on various NRC committees including one concerning water security planning for the Environmental Protection Agency (EPA) and another concerned with science and technology for countering terrorism. He was elected to the National Academy of Engineering in 2006. He received his B.S.C.E. in civil engineering from the University of California and his M.Sc. and Ph.D. (1972) in civil engineering from the Massachusetts Institute of Technology.

Vicki M. Bier holds a joint appointment as Professor in the Department of Industrial and Systems Engineering and the Department of Engineering Physics at the University of Wisconsin-Madison, where she has directed the Center for

Human Performance and Risk Analysis since 1995. Her current research interests include the application of decision analysis, risk analysis, game theory, and related methods to homeland security and critical infrastructure protection. As such, she brings to the committee a wealth of knowledge about DHS programs and models. Other interests include the use of accident precursors or near misses in probabilistic risk analysis, the use of expert opinion, and methods for effective risk communication, both to decision makers and to the general public. She served as the engineering editor for *Risk Analysis* from 1997 through 2001 and has been a councilor of both the Society for Risk Analysis and the Decision Analysis Society. Dr. Bier has served as a member of the Radiation Advisory Committee of the U.S. Environmental Protection Agency's Science Advisory Board. She resigned from the committee on July 1, 2009, when she began to perform research supported by the Department of Homeland Security. She received a Ph.D. in Operations Research from the Massachusetts Institute of Technology (MIT) and a B.S. in Mathematical Sciences from Stanford University.

Robin Cantor is principal at Exponent Consulting. Dr. Cantor specializes in environmental and energy economics, applied economics, statistics, risk management, and insurance claims analysis. Prior to joining Exponent, she led the liability estimation practice at Navigant Consulting and assisted companies and financial institutions with analysis to better understand asbestos and other product liability exposures. Other positions she has held include principal and managing director of the Environmental and Insurance Claims Practice at LECG, LLC, program director for Decision, Risk, and Management Sciences, a research program of the National Science Foundation (NSF); and senior research appointments at Oak Ridge National Laboratory. She was president of the Society for Risk Analysis in 2002, and from 2001-2003 she served as an appointed member of the Research Strategies Advisory Committee of the EPA's Science Advisory Board. Dr. Cantor received her B.S. in mathematics from Indiana University of Pennsylvania and Ph.D. in economics from Duke University.

Timothy A. Cohn is a senior scientist with the U.S. Geological Survey (USGS). He served as hazards theme coordinator in the director's office in the agency's headquarters. Part of his duties involved interaction with other federal agencies, including the Federal Emergency Management Agency (FEMA), concerning science and policy matters related to the host of natural disasters in which the federal government has responsibilities. He is also a hydrologist in the USGS Office of Surface Water. He has extensive experience and expertise in statistical hydrology, especially the estimation of flood risks. Dr. Cohn received his B.A. in mathematics from Swarthmore College and his M.S. and Ph.D. (1983) in water resources systems engineering from Cornell University.

Debra Elkins resigned from the committee on December 7, 2009 when she took a position with the DHS's Office of Risk Management and Analysis. Dr.

Elkins was formerly with the Quantitative Research and Analytics group of Allstate Insurance Company in Northbrook, Illinois. Her research interests include risk modeling for enterprise operations, manufacturing and supply chain vulnerability analysis and disruption consequence modeling, decision-making under uncertainty, computational issues in stochastic processes, applied probability and statistics, and enterprise-scale simulation. Prior to joining Allstate in 2007, Dr. Elkins carried out similar functions with General Motors R&D. She has served as an industry technical expert for DHS and NSF, and she has briefed the U.S. National Defense University/Industrial College of the Armed Forces on global manufacturing and supply chain risks. Dr. Elkins received a B.S. in Mathematical Physics from Sweet Briar College in Virginia, and was elected to Phi Beta Kappa. She received her Ph.D. in Industrial Engineering–Operations Research from Texas A&M University. She recently served on the NRC's Board on Mathematical Sciences and Their Applications.

Ernest R. Frazier, Sr., is president of Countermeasures Assessment and Security, Camden, N.J., which is a security consulting firm for government and private industry. Prior to his current position, Mr. Frazier directed the public safety division of New Castle County in Delaware where he managed nationally accredited sworn law enforcement agency, emergency communications, 911, fire and ambulance, emergency medical paramedic services, and emergency preparedness and response functions. At the time of the September 11, 2001, attacks on the United States, he was senior vice president and chief of security for Amtrak overseeing security services to more than 24 million annual rail passengers and 20,000 employees and corporate emergency preparedness and response functions. He holds a B.A. in business law from Temple University and a J.D. from Rutgers School of Law.

Katherine Hall is director of strategy and plans for global analysis at BAE Systems. Prior to joining BAE, she directed the analysis and production section of the National Geospatial-lntelligence Agency (NGA), which is responsible for the management and strategic direction of several thousand intelligence analysts. Ms. Hall led the NGA's Integrated Operations Center in Denver which was cited by the Director of National Intelligence as a model of interagency cooperation. Prior to moving to NGA, she was a senior intelligence officer with the Central Intelligence Agency (CIA). As part of CIA's Office of Military Support, she directed CIA's representative to NORAD/USSPACECOM, where she acted as a senior intelligence advise to the commander. Ms. Hall was also a national intelligence officer and head of the National Intelligence Council's Analytic Group, an organization of senior intelligence officers responsible for the production of national estimates. She personally drafted several national intelligence estimates and with others was the developer of the first U.S. government model to estimate the spread and impact of AIDS. She also served in several senior positions in CIA's Directorate of Intelligence such as deputy director of the CIA's Office of Asian Pacific and Latin American Analysis and director of

the Office of Africa and Latin America. She began her career as a military and weapons analyst. Ms. Hall received her B.A. in history and physics from Mount Holyoke College and her M.A. in international relations from George Washington University.

Roger E. Kasperson (NAS) is a research professor and distinguished scientist in the Graduate School of Geography at Clark University. He has published widely in the areas of risk analysis, risk communication, global environmental change, risk and ethics, and environmental policy. Dr. Kasperson was elected a member of the National Academy of Sciences in 2003 and the American Academy of Arts and Sciences in 2004 for his work on extending scientific assessment of risk into the social realm, creating a theory for the social amplification and attenuation of risk—with practical applications in analyzing national cultures and multinational corporations, moral bases of technological choice, and environmental degradation. He has been a consultant or advisor to numerous public and private agencies on energy and environmental issues and has served on various NRC committees and the Council of the Society for Risk Analysis. From 1992 to 1996, he chaired the International Geographical Union Commission on Critical Situations/Regions in Environmental Change. Currently, he serves on the NRC's Committee on Human Dimensions of Global Change Committee and the Committee on Strategic Advice for the Climate Change Program of the U.S. National Research Council. Dr. Kasperson has a Ph.D. in geography from the University of Chicago.

Donald Prosnitz is currently a consultant and senior principal researcher (adjunct) at RAND Corporation. His studies at RAND concentrate on the utilization of technology to solve national and homeland security issues. Dr. Prosnitz was previously the deputy associate director (programs) for nonproliferation, homeland and international security at Lawrence Livermore National Laboratory, where he was responsible for overseeing all of the directorate's technical programs. He received his B.S. from Yale University and his Ph.D. in physics from the MIT. He then spent two years as an assistant professor in the Engineering and Applied Science Department at Yale before joining Lawrence Livermore National Laboratory as an experimental laser physicist. Over the next three decades, he conducted research on lasers, particle accelerators, high-power microwaves, free-electron lasers, and remote sensing, and he managed the design, construction, and operation of numerous research facilities. In 1990, he was awarded the U.S. Particle Accelerator Award for Achievement in Accelerator Physics and Technology. In 1999, Dr. Prosnitz was named the first chief science and technology adviser for the Department of Justice (DOJ) by Attorney General Janet Reno. In this newly created position, he was responsible for coordinating technology policy among DOJ's component agencies and with state and local law enforcement entities on science and technology projects and programs. In 2002, he was named a fellow of the American Physical Society (APS); he is currently the chair of the APS Forum on Physics and Society and was until re-

cently a member of the NRC's Board on Chemical Sciences and Technology.

Joseph V. Rodricks is a principal of ENVIRON International, a technical consulting firm, and a visiting professor at the Johns Hopkins University Bloomberg School of Public Health. He is a toxicologist specializing in the evaluation of health risks associated with human exposure to chemical substances of all types. Dr. Rodricks came to consulting after a 15-year career as a scientist at the U.S. Food and Drug Administration (FDA). He joined FDA's Bureau of Science after receiving degrees in chemistry (MIT) and biochemistry (University of Maryland). His experience extends from pharmaceuticals, medical devices, and foods, to occupational chemicals and environmental contaminants. He currently serves on the NRC's Board on Environmental Studies and Toxicology and has served on many committees of the NRC and the Institute of Medicine, including the committees that produced the seminal work *Risk Assessment in the Federal Government* (1983) and the recent study *Science and Decisions: Advancing Risk Assessment*. He is author of the widely used text *Calculated Risks*.

Mitchell J. Small is the H. John Heinz III Professor of Environmental Engineering in the Departments of Civil and Environmental Engineering and of Engineering and Public Policy at Carnegie Mellon University. Dr. Small's research focuses on mathematical modeling of environmental quality, including statistical methods and uncertainty analysis, human exposure modeling, and environmental decision support. Recent applications include sensor placement to protect water distribution systems and leak detection at CO_2 geologic sequestration sites. He has served on several NRC committees, including the Committee on Risk Characterization and the Committee on Environmental Remediation at Naval Facilities. Dr. Small is an associate editor for the journal *Environmental Science & Technology* and a fellow of the Society for Risk Analysis. He received his B.S. in civil engineering and public affairs from Carnegie Mellon University and his M.A. and Ph.D. (1982) in environmental engineering from the University of Michigan.

Monica Schoch-Spana is a medical anthropologist, senior associate with the Center for Biosecurity of the University of Pittsburgh Medical Center (UPMC), and assistant professor in the School of Medicine's Division of Infectious Diseases. Dr. Schoch-Spana has led research, education, and advocacy efforts to encourage greater consideration by authorities of the general public's capacity to confront bioattacks and epidemics constructively—a realm she has termed "the people's role in biodefense." She recently chaired the Working Group on Citizen Engagement in Health Emergency Planning and was the principal organizer of the 2006 U.S.-Canada summit on Disease, Disaster, and Democracy—The Public's Stake in Health Emergency Planning. In 2003, she organized the national summit Leadership During Bioterrorism: The Public as an Asset, Not a Problem and chaired the Working Group on Governance Dilemmas

in Bioterrorism Response that issued consensus recommendations to mayors, governors, and top health officials nationwide in 2004. Over the last 10 years, Schoch-Spana has briefed numerous federal, state, and local officials as well as medical, public health, and public safety professionals on critical issues in biosecurity. She has served on several NRC committees, and is presently with the National Academies' Disasters Roundtable. She is a faculty member of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a university-based center of excellence supported by DHS. Dr. Schoch-Spana received her B.A. from Bryn Mawr College and her Ph.D. in cultural anthropology from Johns Hopkins University.

Ellis M. Stanley, Sr., is director of Western Emergency Management Services at Dewberry, in Los Angeles. Prior to that, he was general manager of the City of Los Angeles Emergency Preparedness Department. He has directed emergency management programs around the United States for 25 years and has also served as a county fire marshal, fire and rescue commissioner, and county safety officer. Mr. Stanley was president of the International Association of Emergency Managers, the American Society of Professional Emergency Planners, and the National Defense Transportation Association. He is the City of Los Angeles' representative in the Cluster Cities Project of the Earthquake Megacities Initiative—a project that fosters sharing of knowledge, experience, expertise, and technology to reduce risk to large metropolises from earthquakes and other major disasters. Mr. Stanley is also an adviser to the Multidisciplinary Center for Earthquake Engineering Research. He was previously a member of the NRC's Natural Disasters Roundtable. He has a B.S. (1973) in political science from the University of North Carolina at Chapel Hill.