TRANSPORTATION RESEARCH BOARD
*OF THE NATIONAL ACADEMIES*

**SPECIAL REPORT 270**

# DETERRENCE, PROTECTION, AND PREPARATION

## THE NEW TRANSPORTATION SECURITY IMPERATIVE

SPECIAL REPORT 270

# DETERRENCE, PROTECTION, AND PREPARATION

## THE NEW TRANSPORTATION SECURITY IMPERATIVE

PANEL ON TRANSPORTATION
Committee on Science and Technology for Countering Terrorism

TRANSPORTATION RESEARCH BOARD
*OF THE NATIONAL ACADEMIES*

Transportation Research Board
Washington, D.C.
2002
www.TRB.org

# Transportation Research Board Special Report 270

Transportation Research Board publications are available by ordering individual publications directly from the TRB Business Office, through the Internet at www.TRB.org or national-academies.org/trb, or by annual subscription through organizational or individual affiliation with TRB. Affiliates and library subscribers are eligible for substantial discounts. For further information, contact the Transportation Research Board Business Office, 500 Fifth Street, NW, Washington, DC 20001 (telephone 202-334-3213; fax 202-334-2519; or e-mail TRBsales@nas.edu).



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 competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to the procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

## Library of Congress Cataloging-in-Publication Data

National Research Council (U.S.). Committee on Science and Technology for Countering Terrorism. Panel on Transportation.

Deterrence, protection, and preparation : the new transportation security imperative / Panel on Transportation: Science and Technology for Countering Terrorism.

p. cm.—(Special report ; 270)

"Transportation Research Board, National Research Council."

ISBN 0-309-07710-9

1. Terrorism—Prevention—Government policy—United States. 2. Transportation—Security measures—United States. I. National Research Council (U.S.). Transportation Research Board. II. Title. III. Special report (National Research Council (U.S.). Transportation Research Board) ; 270.

HV6432 .N385 2002
363.12—dc21 2002074037

# 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. On 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. Bruce M. Alberts 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 achievements of engineers. Dr. William A. Wulf 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, on 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 the Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation by stimulating and conducting research, facilitating the dissemination of information, and encouraging the implementation of research results. The Board's varied activities annually engage more than 4,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

**www.national-academies.org**

## Committee on Science and Technology for Countering Terrorism

Lewis M. Branscomb, Harvard University, *Co-chair*
Richard D. Klausner, Bill & Melinda Gates Foundation, *Co-chair*
John D. Baldeschewieler, California Institute of Technology
Barry R. Bloom, Harvard School of Public Health
L. Paul Bremmer III, Marsh and McLennan Companies, Inc.
William F. Brinkman, Lucent Technologies (retired)
Ashton B. Carter, Harvard University
Charles B. Curtis, Nuclear Threat Initiative
Mortimer L. Downey, PBConsult
Richard L. Garwin, Council on Foreign Relations
Paul H. Gilbert, Parsons Brinckerhoff Quade and Douglas
M. R. C. Greenwood, University of California, Santa Cruz
Margaret A. Hamburg, Nuclear Threat Initiative
William Happer, Princeton University
John Hennessy, Stanford University
Joshua Lederberg, Sackler Foundation at the Rockefeller University
Thomas C. Shelling, University of Maryland
Maxine F. Singer, Carnegie Institution of Washington
Neil J. Smelser, University of California, Berkeley (retired)
Philip M. Smith, McGeary & Smith
P. Roy Vagelosi, Merck and Co., Inc. (retired)
Vincent Vitto, Charles Stark Draper Laboratory, Inc.
George M. Whitesides, Harvard University
R. James Woolsey, Jr., Shea & Gardner

## Committee on Science and Technology for Countering Terrorism: Panel on Transportation

Mortimer L. Downey, PBConsult, *Panel Chair*
H. Norman Abramson, Southwest Research Institute
Lisa M. Bendixen, ICF Consulting Services, LLC
Anthony J. Broderick, Federal Aviation Administration (retired)
Noel K. Cunningham, Port of Los Angeles
John J. Fearnsides, George Mason University
CDR Stephen E. Flynn, U.S. Coast Guard
Francis B. Francois, American Association of State Highway and Transportation Officials (retired)
Ernest R. Frazier, Sr., National Railroad Passenger Corporation
Robert E. Gallamore, Northwestern University
Henry L. Hungerbeeler, Missouri Department of Transportation
Brian M. Jenkins, RAND Corporation
Daniel Murray, ATA Foundation
Edmond L. Soliday, United Airlines (retired)
Richard A. White, Washington Metropolitan Area Transit Authority
James A. Wilding, Metropolitan Washington Airports Authority

### National Research Council Staff

Thomas R. Menzies, Jr., Senior Program Officer, Transportation Research Board

# Preface

The September 11, 2001, attacks galvanized the nation to strengthen its counterterrorism defenses. Immediately following the attacks, the presidents of the National Academy of Sciences, National Academy of Engineering, and Institute of Medicine wrote to President Bush offering the advice of the National Academies on how best to harness the country's science and technology capacity to meet critical security and antiterrorism needs.

In December 2001, the National Academies appointed a committee of 24 of the country's leading scientific, engineering, medical, and public policy experts to offer counsel on an integrated science and technology plan for combating terrorism. To supplement the knowledge of its members, the committee convened eight panels with expertise in specific topic areas, from the chemical and biological disciplines to the domains of energy, information technology, and transportation. Mortimer L. Downey, a member of the main committee, led the Transportation Panel, which comprised 17 experts in transportation operations, engineering, and administration; research and technology; and safety, security, and law enforcement.

The main committee's report, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, was released on June 25, 2002. The committee recommends a strategy whereby the nation's scientific and engineering capacity can be strengthened and brought to bear in the fight against terrorism. *Making the Nation Safer* synthesizes the contributions of the eight expert panels into chapters, each containing specific research and policy recommendations. The Transportation Panel's contribution (Chapter 7 of *Making the Nation Safer*) is reprinted in this Transportation Research Board (TRB) Special Report to provide for more direct dissemination within the transportation research, operations, and policy-making communities. The executive summary of *Making the Nation Safer* is reprinted in the appendix to the present report.

The Transportation Panel convened twice and communicated by e-mail and conference calls over a 5-month period. During its two meetings, the panel received briefings on the security-related research and development (R&D) activities of most of the modal agencies within the U.S. Department of Transportation. Thanks are due to Steven Ditmeyer, Federal Railroad Administration; James O'Steen and Frits Wybenga, Research and Special Programs Administration; David Price and Michael Trentacoste, Federal Highway Administration; Douglas McKelvey, Federal Motor Carrier Safety Administration; Lyle Malotky, Federal Aviation Administration; William Siegel, Federal Transit Administration; Captain James Evans, U.S. Coast Guard; and Richard John and Michael Dinning, Volpe National Transportation Systems Center. Thomas G. Day, Vice President for Engineering, U.S. Postal Service, also joined in the panel's deliberations, making valuable contributions to the discussion.

The panel met with other experts outside government as well. Joseph Del Balzo, JDA Aviation Technology Solutions, reviewed technological possibilities for computerized prescreening of passenger traffic to enhance aviation security. Thomas Hartwick discussed the state of technologies and systems with the potential to improve aviation security. Raja Parasuraman, Catholic University, and Victor Riley, Honeywell Inc., addressed the role of human factors in the design, development, and deployment of security technologies and systems. The panel extends its gratitude to all four for their valuable contributions.

In addition, the panel wishes to thank Stephen McHale, Deputy Under Secretary for Transportation Security, and Paul Busick, Acting Associate Administrator for Civil Aviation Security. Both briefed the panel on the status of the newly created Transportation Security Administration and welcomed the ideas and comments of panel members.

The panel's contribution was reviewed as part of the main committee's report by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the insti-

tution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

The full listing of the reviewers of the main committee's report is provided in *Making the Nation Safer*. Several of these reviewers were selected because of their transportation expertise. Special appreciation is expressed to the following reviewers: Lillian C. Borrone, Port Commerce Department, Port Authority of New York and New Jersey (retired); Lester A. Hoel, L. A. Lacy Distinguished Professor of Engineering, University of Virginia; Donald E. Brown, Professor and Chair, Department of Systems Engineering, University of Virginia; and Joseph M. Sussman, Professor of Civil and Environmental Engineering and Engineering Systems, Massachusetts Institute of Technology. Although these individuals provided many constructive comments and suggestions, they were not asked to endorse findings and conclusions, nor did they see the final document before its release.

The review was overseen by R. Stephen Berry, James Franck Distinguished Service Professor Emeritus, University of Chicago, and Gerald P. Dinneen, Retired Vice President of Science and Technology, Honeywell Inc. 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 carefully considered. Responsibility for content rests entirely with the authors and the institution.

Thomas R. Menzies, Jr., managed the panel's work under the guidance of the panel and the supervision of Stephen R. Godwin, Director of Studies and Information Services, TRB. Suzanne Schneider, Associate Executive Director of TRB, assisted with the review process. This manuscript was edited by Rona Briere and prepared for publication by Alisa Decatur under the supervision of Nancy Ackerman, Director, Reports and Editorial Services, TRB. Jocelyn Sands directed project support staff. Special thanks go to Amelia Mathis and Frances Holland for assistance with meeting arrangements and correspondence with the panel.

# Dedication

The Transportation Panel is indebted to the work of earlier NRC committees. In particular, the 1999 NRC report *Improving Surface Transportation Security: A Research and Development Strategy* helped shape the panel's thinking on the need for a systems approach to transportation security and a congruent research and development strategy. A key member of the NRC committee that produced *Improving Surface Transportation Security*, Fred V. Morrone, Director of Public Safety and Superintendent of Police for the Port Authority of New York and New Jersey, died on September 11, 2001, while responding to the World Trade Center attacks. The panel undertook its effort in memory of Superintendent Morrone.

# CONTENTS

# Executive Summary

The nation's vast air, land, and maritime transportation systems are marvels of innovation and productivity, but they are designed to be accessible, and their very function is to concentrate passenger and freight flows in ways that can create many vulnerabilities for terrorists to exploit. Prospects for defending against each of these vulnerabilities through traditional means, such as "guards, guns, and gates," are dim. The transportation sector is simply too large and the threats faced too diverse and ever-changing for such blanket approaches to work. Moreover, if applied in the large and diffuse transportation sector, these approaches run the risk of creating a diluted and patchwork collection of poorly connected defenses that disperse security resources while leaving many vulnerabilities unprotected against a terrorist attack.

Transportation security can best be achieved through coherent security systems that are well integrated with transportation operations and are deliberately designed to deter terrorists even as they selectively guard against and prepare for terrorist attacks. In particular, layered security systems, characterized by an interleaved and concentric set of security features, have the greatest potential to deter and protect. Layered systems cannot be breached by the defeat of a single security feature—such as a gate or guard—as each layer provides backup for the others, so that impermeability of individual layers is not required. Moreover, the interleaved layers can confound the would-be terrorist. Calculating the odds of breaching a multitiered system of defense is far more difficult than calculating the odds of defeating a single, perimeter protection.

When integrated well with transportation services and functions that confer other benefits, such as enhanced safety and service quality, layered systems are even more likely to be deployed and sustained over time. Multi-use systems—for instance, systems that benefit transportation operators and users

by monitoring the condition of infrastructure and location of vehicles, baggage, and cargoes—are apt to be maintained and continually adapted to the changing transportation environment. A combination of public leadership and private incentives is therefore essential to the deployment of such dynamic, built-in security systems.

The dangers of not taking such a systematic approach to security were manifest in the aviation sector on September 11. Commercial aviation has been the subject of hostile attacks for many years. Each new attack has prompted the advent of new technologies, procedures, and rules, yielding an assortment of measures each intended to address a discrete threat in a particular way. Whether to find bombs in suitcases or to interdict hijackers carrying handguns, each has been deployed with a single security objective in mind. By defeating one such perimeter defense—passenger screeners intended to intercept handguns—the September 11 attackers were able to defeat the entire security regime. And after the attacks, federal policymakers, seeking to secure commercial aviation and regain public confidence in air travel, did not have a well-designed security system in place that could be assessed methodically to identify gaps that needed to be filled.

To be sure, reshaping transportation security approaches to create layered systems of deterrence and protection will not be easy. Security planners will need to question many existing security rules, methods, technologies, and institutional relationships. And they will need the support of sound research and evaluation, as well as the cooperation and collaboration of the many public, private, and foreign entities that will have to implement the systems.

In the wake of the September 11 attacks, Congress created the Transportation Security Administration (TSA) within the U.S. Department of Transportation (DOT).[1] TSA was assigned a set of aviation security responsibilities with strict deadlines—from the federalizing of all airport security screeners to the deployment of air marshals on airliners and the installation of explosive detection systems at all commercial airports. Previously, civil aviation security was overseen and regulated by the Federal Aviation Administration,

[1] Aviation and Transportation Security Act of 2001 (Public Law 107-71).

but operational and financial responsibilities were shared among the private airlines and the airports owned by state and local governments. Security for other modes of land and maritime transportation was, and remains largely today, the responsibility of state and local law enforcement authorities, the many public and private entities that own and operate transportation infrastructure and assets, and various federal agencies responsible for port and border security. In creating TSA, Congress added a new dimension to the federal role by giving the agency explicit responsibility for security in all modes of transportation and for the development of policies, strategies, and plans for addressing transportation security threats.

Still in its formative stage, TSA presents an unprecedented opportunity to build security into the nation's transportation sector in a more systematic fashion. Indeed, Congress has chartered TSA to take on such a strategic role. Compelled by statute to act quickly in enhancing civil aviation security, TSA is now beginning to examine the security needs of all transportation modes and to define its own role in meeting those needs. The following counsel is offered to TSA as it moves forward in fulfilling this vital strategic responsibility.

## A Strategic Research and Planning Role for TSA

***TSA should establish a strategic research and planning office—attuned to, but distinct from, the agency's operational and enforcement responsibilities—that will work closely with DOT, the modal agencies, other federal agencies, state and local governments, and other elements of the public and private sectors on security system research, planning, and deployment.***

Having a strong analytic capability to undertake systems planning and risk assessment, this recommended office could

- Devise and evaluate promising security system concepts in collaboration with public- and private-sector owners, operators, and users, and through the application of operations research and human factors expertise;

- Ensure that gaps do not exist in security planning and preparation because of the narrow purview of modal agencies and transportation operators and users;
- Encourage the explicit inclusion of security objectives in transportation planning processes and in the design of vehicles, facilities, and operating systems;
- Advise metropolitan governments and transportation agencies on the need to develop integrated regional emergency response plans, and advise local and state transportation agencies, public transit authorities, and related entities on how to reshape their administrative structures so as to give security prominence in their planning and decision making;
- Explore ways in which security features can be encouraged, and market-related and institutional barriers to the deployment of security measures can be overcome;
- Work with other countries and international standards-setting bodies to exchange information about international shipments, coordinate security measures and overall system strategies, and collaborate in research and development (R&D) activities; and
- Develop a critical research agenda in support of transportation security systems.

To be effective and trusted, TSA must be more than just a regulatory and enforcement arm of DOT; it must find ways to share needed expertise and information and to work constructively with those entities–from modal agencies to public- and private-sector transportation system operators–entrusted with fielding security solutions. A strategic research and planning office within TSA, unencumbered by rulemaking, enforcement, and operational responsibilities, could offer these needed services.

## An R&D Role That Builds Connections and Extends Beyond Transportation

***TSA should collaborate with the public and private sectors to build a strong foundation of research on human factors and transportation opera-***

***tions, and to make the evaluation of security system concepts a central element of its collaborative research program. TSA should establish an in-house research capacity to undertake such concept evaluations and to support its own large security operations and technology acquisition programs. At the same time, the agency should adopt a broader, architect-like role in promoting and marshaling R&D to advance these security systems, especially by tapping into the security-related R&D of other government agencies, the broader transportation community, universities, research institutions, and the private sector.***

In support of security systems analysis and planning, as well as its operational and technology acquisition programs, TSA must have both its own research capacity and the ability to work with and draw on expertise from within and outside the broader transportation community. Within DOT, the individual modal agencies and the Volpe National Transportation Systems Center offer important resources for systems-level research and technology development. By viewing the R&D activities of the modal agencies, as well as those of state and local transportation agencies, in such a comprehensive way, TSA can determine where targeted additional R&D investments have the potential to yield large benefits, and can orchestrate means of encouraging such investments. In so doing, TSA can better leverage the transportation sector's R&D investments to ensure that they have strong security relevance. One area in which TSA can play an important role is in ensuring that the nation's human factors expertise is integrated into all aspects of transportation security planning, research, technology development, and operations.

Much of this and other needed research and technology development capacity will be available outside the transportation community, in the nation's universities and research institutions, with support from much larger R&D sponsors, such as the Department of Defense, the National Institutes of Health, and the National Science Foundation. By making the needs and parameters of transportation security systems more widely known, TSA can help identify and shape research and technology development activities that are outside the transportation realm, but have potential transportation security applications.

## A Technology Guidance and Evaluation Capacity

***TSA should create a technology guidance, evaluation, and clearinghouse capacity to provide developers with performance goals for their products, and to advise transportation system operators on security-related technologies that are available or under development.***

At the moment, there is a great deal of interest within the public and private sectors in developing and employing technologies for transportation security. As a result, the potential exists for much effort to be expended on the development of technologies that are not well suited to transportation settings or that are incompatible with security systems. Thus, as it proceeds in identifying appropriate security systems for each transportation mode, TSA should be prepared to offer guidance to commercial developers on the technological capabilities that are most appropriate. By articulating these performance needs and parameters, TSA can provide technology developers with a clearer target for their R&D efforts. By implementing this recommendation, TSA can also give transportation system owners and operators a better sense of which technologies and processes will work, and where opportunities may exist to collaborate with researchers and developers to advance promising technologies and concepts.

## Need for Unconventional Thinking on Threats and Responses

What was demonstrated on September 11 is that transportation systems and assets can be misused by terrorists in ways that can be difficult to anticipate and overlooked in day-to-day efforts to ensure transportation security. The advent of TSA should be helpful in increasing the attention paid to security within the transportation community, but perhaps not in overcoming the bias of viewing transportation assets and operations within functional domains—and securing them as such. Given the size, scope, and ubiquity of the transportation sector, coupled with its myriad owners, operators, and users, many

opportunities exist for terrorists to exploit components of transportation systems in novel ways unanticipated by those traditionally responsible for transportation security. By and large, transportation systems are regulated at the mode-specific level, and the entities that own and use them are organized for the efficient provision of specific services. Yet terrorists are actively seeking to exploit new threat vectors that lie beyond such conventional perceptions of order. Terrorists may not view individual transportation assets, infrastructure, and services in such self-contained and functionally oriented ways, but rather as components and tools of other systems—much as jet airliners and mailed letters were used as weapon delivery systems.

A broader-based understanding of terrorist threats that involve transportation and its intersection with other domains is clearly needed if the transportation community is to do its job in keeping its systems from being exploited again to such tragic effect. Recognizing that such an analytical need exists more generally, the report of the National Academies on *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*[2] urges the creation of a Homeland Security Institute—an entity outside normal organizational settings whose sole mission would be to explore and systematically assess terrorist threats, probable responses and reactions, and ensuing consequences.

[2] The executive summary of *Making the Nation Safer* is reprinted in the appendix to the present report.

# 1
# Introduction and Overview

Transportation vehicles and facilities, from airliners to rail terminals, are recurrent targets of terrorist attacks, hijackings, and sabotage.[1] The September 11 hijackers added a new dimension to this linkage by turning four jet airliners into guided missiles targeting large buildings. Only a few weeks later, the mailer of anthrax capitalized on the anonymity and reach of the nation's postal system to deliver this bioweapon to targeted individuals in the national media and the federal government (and to random individuals along the way). Given their prominence in past acts of terrorism, there is good reason to believe that the nation's transportation systems will be exploited again in attacks of potentially equal or greater consequence.

The characteristics of transportation systems make them especially vulnerable—and therefore attractive—to terrorists. Passenger vehicles and facilities often contain large numbers of people in enclosed spaces. Vehicles moving rapidly—whether in the air, on the surface, or below ground—are in precarious and fragile positions; much damage can be done with the introduction of a relatively small and well-placed force. Certain elements of the transportation infrastructure, such as U.S.-flag carriers and landmark bridges and tunnels, are symbolic to Americans, adding further to their appeal as terrorism targets.

Many transportation facilities and structures are strategically important, serving as key nodes in networks and corridors that handle large volumes of

[1] For a description of the range and nature of terrorist attacks in public surface transportation, see Jenkins (1997; 2001). A report of the National Research Council (NRC 1999) also describes the characteristics of previous terrorist attacks on surface transportation.

people, goods, and services, including military movements. Moreover, transportation systems are international in scope and intertwined with economic and social activities. For instance, a few seaports handle a major share of the goods moved in international trade, and commuter and rapid rail transit services are the circulatory systems of urban environments, critical to the functioning of some of the largest U.S. cities. Hence disruptions to these systems can have potentially far-reaching and long-lasting economic and social effects.

To be sure, transportation vehicles and containers can be tempting weapons in and of themselves, as most vehicles are powered by flammable fuels, and some carry bulk shipments of extremely hazardous chemicals. By their very nature, these vehicles are highly mobile, and thus capable of being used to access a range of targets quickly. They are also ubiquitous, moving unnoticed within industrial locations and major population centers and across borders. Their mobility, range, and omnipresence make transportation vehicles a ready means of delivering terrorist weapons, from conventional explosives to unconventional chemical, biological, and radiological agents. And in the case of mail and express package services, the weapons can be carried into nearly every household, business, and government office in the country.

In Chapter 2, the characteristics of transportation systems are described, and the features of security systems that take these characteristics into account are reviewed. The kinds of research that will be required to support the development and deployment of such security systems are delineated in Chapter 3. Advice to TSA on strategic research and planning is presented in Chapter 4, and concluding observations are made in Chapter 5.

After the September 11 attacks, President Bush created the Office of Homeland Security. Soon afterward, Congress passed the Aviation and Transportation Security Act, which established an Under Secretary for Transportation Security and a Transportation Security Administration (TSA) within the U.S. Department of Transportation (DOT).[2] Civil aviation security had previously been overseen and regulated by the Federal Aviation

[2] The Aviation and Transportation Security Act (Public Law 107-71) was signed by President Bush on November 19, 2001.

Administration (FAA), but operational and financial responsibilities rested with the private airlines and the airports, owned by state and local governments. Security in other modes of land and maritime transportation had been, and largely remains today, the responsibility of state and local law enforcement authorities, the many public and private entities that own and operate transportation systems, and various federal agencies responsible for port and border security. TSA should take the lead in identifying coherent security systems for each mode of transportation, to work with the private and public sectors in this country and abroad in deploying these systems, and to further the development of supporting expertise and technologies.

## REFERENCES

### ABBREVIATION

NRC National Research Council

Jenkins, B. M. 1997. *Protecting Surface Transportation Systems and Patrons from Terrorist Activities: Case Studies of Best Security Practices and a Chronology of Attacks*. Report 97-4. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose State University, San Jose, Calif.

Jenkins, B. M. 2001. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*. Report MTI-01-14. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose State University, San Jose, Calif.

NRC. 1999. *Improving Surface Transportation Security: A Research and Development Strategy*. National Academy Press, Washington, D.C.

# 2

# Transportation System Characteristics and Their Implications for Security

Several common characteristics of transportation systems make it likely that certain kinds of security strategies will be most suitable. These characteristics, along with their implications for security strategies, are discussed in this chapter.

## Key Transportation System Characteristics

Security strategies must be suited to the systems to be secured and defended. The salient common characteristics of transportation systems are reviewed below.

### Open and Accessible

Designed and organized for the efficient, convenient, and expeditious movement of large volumes of people and goods, transportation systems must have a high degree of user access. In some cases—highways, for example—access is almost entirely open. Many transportation facilities, such as train stations, are public places, open by necessity. In other cases, such as commercial aviation, access is more limited, but still not fully closed; access to most airport lobbies, ticket lines, and baggage check-in areas remains unrestricted. Moreover, much of the transportation infrastructure, from airports to highway and rail bridges, was designed and built long before concerns about security and terrorism had arisen. Fully integrating security within the transportation sector will take many decades as long-lived assets are gradually modified and replaced.

## Extensive and Ubiquitous

Transportation systems require vast amounts of physical infrastructure and assets.[1] The U.S. highway system consists of 4 million interconnected miles of paved roadway, including more than 45,000 miles of Interstate freeway and 600,000 bridges. Freight rail networks extend for more than 300,000 miles, and commuter and urban rail systems cover some 10,000 miles. Even the more contained civil aviation system has around 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks also contain many other fixed facilities, such as terminals, navigation aids, switchyards, locks, maintenance bases, and operation control centers.

Most of this infrastructure is unguarded and sometimes unattended. Distributed over the networks are millions of vehicles and containers. These vehicles and containers are repeatedly moved from one location to another, complicating the task of monitoring, safeguarding, and controlling them.

## Emphasis on Efficiency and Competitiveness

Although much of the transportation infrastructure in the United States is owned by the public sector, the development of this infrastructure has been driven largely by the demands of private users. Widespread use of private cars and motor carriers, for instance, has spurred greater investment in the highway system relative to public transit and railroads. Likewise, travel by motor vehicle and airplane displaced demand for intercity passenger rail service in the second half of the 20th century, prompting increased government spending on freeways and airports. The economic deregulation that swept through the transportation sector during the last quarter of the 20th century has led to even greater emphasis on efficiency as a criterion for transportation investments and, to a certain degree, to a loss of redundancy and excess capacity in the sector as a whole. The dynamism of the U.S. transportation sector is unmatched in the world, and is a major reason for the nation's high produc-

[1] See Bureau of Transportation Statistics (2000) for more complete statistics on the extent of the U.S. transportation sector. The numbers cited in this subsection are derived mainly from this compendium.

tivity and mobility. Another consequence of the increased emphasis on efficiency, however, is that costly security measures that promise unclear benefits or impede operations are likely to be resisted or eschewed, whereas those that confer economic benefits are apt to be deployed and sustained.

## Diverse Owners, Operators, Users, and Overseers

Much of the physical infrastructure of transportation—from highways and airports to urban rail networks—is owned and administered by the public sector. While the federal government helps fund construction, however, it owns and operates very little of this infrastructure.[2] Most of it is controlled by thousands of state and local governments. Private companies and individuals own some fixed infrastructure (as with freight railroads), but they function mainly as service providers and users, controlling most of the vehicles and containers that use the networks.

These public and private owners and operators are largely responsible for policing and securing the system, with the help of state and local law enforcement authorities and, for movements outside the country, foreign governments and international organizations. In addition to providing financial support for infrastructure (and now security for commercial aviation), the federal government's main role is in promoting and regulating safety and environmental performance, supporting research and system planning, and monitoring and regulating transportation activity at border crossings and international gateways.[3]

## Intertwined with Society and the Global Economy

Trucks of all sizes distribute to retail outlets nearly all the products purchased by consumers and many of the goods and supplies used by industry and government. The rail, pipeline, and waterborne modes, along with large trucks, move products and commodities long distances among utilities, refineries, suppliers,

[2] The major exceptions are the FAA's air traffic control system; roads on federal lands; and certain support services, such as the provision and maintenance of navigation aids (e.g., the Global Positioning System).

[3] A number of federal agencies—the individual modal agencies at DOT, for example, as well as the Department of Agriculture, the Environmental Protection Agency, the Customs Service, the Border Patrol, and the Immigration and Naturalization Service—have specific responsibilities in these areas.

producers, and wholesalers, as well as to and from ports and border crossings. In recent years, these transport modes have greatly increased in efficiency to the point where just-in-time inventorying and manufacturing are commonplace. At the same time, the airlines have become indispensable in connecting our increasingly diffuse nation, and passenger airline service is essential to many areas of the country that depend on tourism and business travel.

At the more local level, a quarter or more of the workers in some large cities commute by public transit, which has come to shape some urban centers, most notably on the eastern seaboard. The U.S. Postal Service delivers mail to every household in the United States and most businesses, totaling some 135 million addresses. The highway system pervades the lives of Americans, who use motor vehicles for most daily activities and for much of their longer-distance vacation travel.

Highways are also used by emergency responders, and both the highway and public transit systems are vital security assets for evacuating people in a crisis and moving critical supplies and services. Consequently, disruptions to transportation networks can have far-reaching effects not only on transportation operations, but also on many other interrelated functions and activities.

## Implications for Security Strategies

Certainly, undermining the ability of terrorists to attack in the first place is a national imperative. Should these efforts fall short, however, the transportation sector must be prepared to defend itself. The characteristics delineated above reveal the great difficulty, indeed impossibility, of defending each potential target or perceived vulnerability individually. The transportation sector is simply too diffuse, diverse, and open—by necessity—for such a defensive approach to work. This does not mean that little or nothing can be done to counter terrorism. Sound security measures can do a great deal. For instance, they can confound and deter terrorist operations, increase the likelihood of terrorists being detected and intercepted, keep casualties and disruptions to a minimum, and reduce panic and reassure passengers in a crisis.[4]

[4] This point is made well by Jenkins (2001) in discussing ways to secure very open public transportation systems.

What the characteristics of the transportation sector suggest is the need for a coherent and systematic approach to security. In particular, such an approach should be shaped by (a) well-designed, layered security systems; (b) an emphasis on adaptability, dual use, and exploitation of existing capabilities; and (c) broad-based and unconventional thinking on terrorist threats and responses.

## Layered Defenses

Transportation security can best be achieved through well-designed security systems that are integrated with transportation operations. The concept of a layered security system, in which multiple security features are connected and provide backup for one another, offers a particular advantage: perfect execution by each element in the system is not crucial, as other elements can compensate for human, technological, or other shortcomings; likewise, enhancements to one element can boost the performance of the system as a whole. Such systems, long used to secure communications and information systems, cannot be breached by defeating a single layer. And because terrorists will find it difficult to calculate the odds of defeating multiple layers, some randomly interleaved, such a system can deter as well as impede terrorist acts.[5]

The dangers of not taking such a coherent, systems approach to security were manifest in the aviation sector on September 11. Commercial aviation has been the subject of hostile attacks for more than 30 years. Each new attack has prompted the advent of more technologies, procedures, and rules—each superimposed on those previously introduced, and designed mainly to prevent a recurrence of similar attacks. Aviation security has not been provided through truly systematic means, but rather through a collection of mostly unrelated measures that have hinged on a very high and sustained level of performance from each, with little or no backup and redundancy. By overcoming a single perimeter defense, such as a metal detector, an attacker could, in effect, overcome the entire security regime.

As noted, the design of security systems must relate closely to the characteristics and functions of the transportation systems they are intended to secure and protect. Technologies and methods developed for one transporta-

[5] The need for a systems approach to security is emphasized in two recent NRC reports (NRC 1999a and 1999b).

tion environment that are modified and applied in an incidental manner to another may yield little more than a patchwork security regime. It may be possible, for example, to prevent future airline attacks by systematically identifying and defending all or most vulnerable points in the aviation system: access to airfields and aircraft can be closely guarded, passengers and their luggage screened with great care, airline and airport workers monitored, and so on. By comparison, the much more open and decentralized maritime and land transportation systems are far less amenable to such a defensive approach. The intensive inspection and screening methods used for air transportation security, for instance, are likely to be impractical for transportation modes that require more convenient user access and have myriad points of entry. Means of deterrence in those systems are therefore critical, as are measures to contain and respond to attacks that do occur. Indeed, it is possible that good mitigation, response, and recovery preparations will themselves dissuade terrorists from attacking these targets, since ensuing damage and disruption may be limited.

The importance of understanding the characteristics of each type of transportation system in designing layered security systems is illustrated by the security system concept for shipping containers presented in Box 2-1. A few large seaport hubs, or megaports, around the world—such as Los Angeles, Long Beach, Newark–Elizabeth, Rotterdam, Hamburg, and Singapore—offer points of leverage for designing a security system that will encourage shippers to load containers in secured facilities and take other, related steps to expedite the movement of their cargoes through the megaports and the logistics stream. Because these ports are so critical to the container shipping industry, such requirements may become the de facto standard in short order. Shippers that choose not to comply may be denied access to the megaports or be subjected to greater scrutiny and its resultant delays.

The narrowing of higher-risk traffic in this manner, supported by such capabilities as data mining and artificial intelligence (as described in more detail in Box 2-1), would allow authorities to make better use of their limited inspection, screening, and enforcement resources. With such a layered security system that began early in the logistics stream, the prospects of a containerized weapon being intercepted before reaching the United States, as well as the chances of the act being deterred in the first place, would likely be greater than under the current system of infrequent container inspections at

**Box 2-1**

## Security System Concept for Shipping Containers

### Background

Intermodal shipping containers carry more than 80 percent of the cargo (as measured in value) moved by ocean liners in international trade. A key benefit of these standardized containers is that they allow for mechanized and automated container handling at transfer points, and they can be moved readily among modes. The sealed containers are also less vulnerable to cargo pilfering and theft. These capabilities have vastly improved the efficiency of ship, train, truck, and terminal operations, reducing the time required for international shipping and enabling more businesses to reduce their warehouse and inventory costs through just-in-time logistics.

In the United States, some 50 ports can handle containers, but few have built a significant business around them because of the large investment required for handling equipment, the need for good connections with highway and rail services, and the economies of scale of warehousing and terminal operations. The three megaports of Los Angeles, Long Beach, and Newark–Elizabeth handle about half of all containers entering and exiting the country. Each of these ports can deal with as many as 10,000 containers in a single day.

The U.S. Customs Service maintains inspectors at each port. Their main job is to classify and appraise goods and collect applicable customs duties; their ancillary functions include the interception of contraband and assistance in enforcing other laws and the regulations of some 40 federal agencies. In most cases, entering containers are cleared with a limited review of documents. Most regular, or known, shippers are precleared, and their shipments and documents are not examined by Customs for as much as 30 days, which may be at the endpoint of their line-haul inland journey by truck or rail. Only about 2 percent of containers are opened and physically inspected at some point in the process. Such inspections

are time-consuming—they usually delay shipments for several days—and add to the costs of shippers and receivers (who often depend on just-in-time service).

## A Threat Scenario

In this scenario, a terrorist purchases a foreign exporter that has a long-standing relationship with U.S. importers. The exporter routinely loads containers at its own facilities. In one of the containers, the terrorist loads a nuclear, chemical, or explosive device that is timed to activate or can be activated remotely. The container is transported unopened through a foreign transshipment port and is then placed along with thousands of other containers on a large container ship destined for a major U.S. port that handles thousands of containers each day. Recognizing the known shipper, U.S. Customs preclears the container with minimal review of documents. Along with thousands of others, the container is transferred to line-haul rail for inland transportation to the point of entry into the U.S. economy.

The full documentation for the container shipment is scheduled to arrive at the U.S. Customs office within 30 days of the container's entry into the country. At any point during this 30-day interval, the deadly device inside can be detonated. Even if intelligence uncovers the plot, there may be no ready way to identify and locate the container, and there is additional concern about other containers that may already be in place around the country or on the way. The federal government is probably compelled to halt the movement of all containers and to isolate thousands of suspect ones. Even if the device is not detonated, commerce is severely affected by the disruption of trade, and the public's confidence in the system of deterrence and interception is eroded.

## Layering of Protection and Deterrence to Lessen the Threat

Security cannot begin and end at the port, but must be integrated into the entire logistics chain. And it must be part of an overall system that

*(continued)*

**Box 2-1** *(continued)* **SECURITY SYSTEM CONCEPT FOR SHIPPING CONTAINERS**

can address multiple threats, instead of an unintegrated series of tactics aimed at addressing one vulnerability at a time. Megaports offer a point of leverage for developing such a systems approach. Containers of most shippers will pass through one or more of these large hub seaports in the United States and abroad. The corresponding port authorities and their governments, therefore, are in a position to impose standardized requirements on shipment security, reporting, and information sharing that would have a near-universal effect on practice throughout the industry. Industry trade associations might be employed to certify compliance with these standards; for instance, a shipper that did not maintain the prerequisites could be denied membership in the association, and nonmember shippers could be refused access to the megaport or have their access severely restricted.

One prerequisite might be that containers be loaded in sanitized facilities that are certified and subject to recertification after a change in ownership. Such facilities, whether at shippers' own locations or those of the freight consolidators, might be secured from unauthorized entry, monitored with surveillance cameras, and equipped with cargo and vehicle scanners. Images from these scanners could be stored with other documentation on a shipment and forwarded to transshipment points or destination ports for comparison when the shipment arrived or during randomized inspections along the way. A tamper-resistant mechanical or electronic seal might be placed on the container at the certified loading facility. Light or temperature sensors might also be placed in the container and set to transmit a signal or sound an alarm if activated by an unexpected opening.

Drivers of vehicles that delivered the containers to the ports might have their identities confirmed through biometric cards and be subject not only to periodic checks on their background, but also to scrutiny, using data-mining techniques, to discern unusual patterns of work and behavior. Microcomputers with transponders might be attached

to the motor system to track its route and shut down the engines upon any veering from the approved course. Meanwhile, manufacturers, importers, and shipping companies could be required to provide authorities with advance notice of the details of their shipments. Such early notification would give inspectors time to assess the validity of the data using artificial intelligence and data-mining capabilities, and to check for anomalies that warranted closer examination.

These capabilities might be provided through a central facility with the necessary expertise and resources; its analysts could then advise inspectors and other enforcement officials on the handling of suspect shipments. Shipments singled out for closer scrutiny, including those from uncertified facilities, could be subject to a variety of nondestructive examinations, from simple reweighing, to vapor and radiation sampling, to radiographic imaging. The container's original scanned image, taken at the original loading facility, could be compared with subsequent scans.

None of these coordinated measures and associated technologies, if fully developed and implemented, would guarantee success in eliminating all of the many vulnerabilities associated with the container logistics system, and the practicality and total costs of such an approach have not been fully evaluated. However, a layered system—even with several imperfect elements—would greatly increase the chances of deterring and intercepting threats. This system would also allow enforcement authorities having intelligence about a threat to take quicker and more effective action to identify suspect containers. Such a systematic and credible security system, which could be improved continually through the adoption of new technologies and techniques, would help reassure the public in the event of an incident, as well as aid in containing disruptions in the critical logistics system by precluding the need for a complete shutdown.

(SOURCES: Flynn 2000a; Flynn 2000b; Flynn 2001; Leeper 1991.)

destination ports and other border crossings. Moreover, it is quite possible that the side benefits of such a system, such as a decline in the use of shipping containers for the movement of contraband and the efficiency-related benefits of a sound shipment tracking system, would by themselves provide strong incentives for participants to continually maintain and enhance the system. A multilayered means of securing shipping containers, which would require considerable international and private-sector collaboration, is in fact being considered by the U.S. Customs Service and other government agencies.[6]

In a different and more varied context, experience with ensuring aviation safety during the past 30 years demonstrates how such a layered approach can indeed be pursued with much success. In commercial aviation, it is noteworthy that one agency has a dominant role in ensuring safety through multiple, coordinated means. FAA is responsible for everything from establishing pilot training requirements to regulating the design and manufacture of aircraft and their components. Safety is ensured through a multipronged process aimed at reducing risks through rigorous standards for flight crew qualification and training, testing and certification of aircraft designs and materials, quality assurance in aircraft production processes, detailed schedules for aircraft maintenance and engine overhauls, a coordinated system for air traffic management, standardized operating procedures, and minimum requirements for runway maintenance and airport rescue and fire services. Coincident failures of these complementary elements are rare, as evidenced by the excellent decades-long safety record of commercial airlines. When failures (or even near-failures) do occur, the safety system is evaluated as a whole, and adjustments made (possibly to multiple elements) to remedy the problem.[7]

Given the outstanding performance of the aviation safety system, it is notable that aviation security, also regulated by FAA until recently, has not

[6] As an example, a new U.S. Customs initiative, the Customs-Trade Partnership Against Terrorism (C-TPAT), represents an effort to build cooperative relationships between governments and shippers that will strengthen overall supply chain and border security. More details on C-TPAT can be found on the U.S. Customs Service website: www.customs.gov/enforcem/tpat.htm.

[7] The importance of a systems approach to aviation security was emphasized by the White House Commission on Aviation Safety and Security (1997), chaired by then–Vice President Gore.

been handled in a similarly holistic fashion. By and large, aviation security tactics and techniques have emerged piecemeal in reaction to a series of individual security failures, beginning with the deployment of magnetometers and X-ray screeners for carry-on luggage following a rash of handgun-enabled hijackings during the 1960s and early 1970s. In this case, the screeners were viewed foremost as protective measures, intended to intercept firearms before they could be brought on board an aircraft. Indeed, year after year, thousands of firearms have been intercepted and confiscated by airport screeners.[8] At the same time, the screeners have also deterred the use of guns by hijackers. Certainly, the September 11 hijackers were reluctant to use handguns. Such deterrence effects, however, have not been evaluated explicitly. More systematic evaluations of security approaches surely would have been helpful in understanding the influence of deterrence and opportunities to strengthen that influence. Indeed, in seeking to regain public confidence in aviation security after September 11, federal policy makers did not have a coherent system in place that could readily be fixed. The absence of such a system prompted Congress to take dramatic and hurried measures, from the federalizing of airport screeners to ambitious deadlines for the deployment of costly and potentially unready explosive detectors.

Deterred from one target, the terrorist may well seek another. But if such deflection is in fact likely, it is all the more important for deterrence measures to be deliberate and well placed to ensure that the most sensitive potential targets are those least appealing to attack.

## Emphasis on Adaptability, Dual Use, and Exploitation of Existing Capabilities

Transportation is a diverse and dynamic enterprise. Transportation operations today, from passenger to cargo systems, are fundamentally different from what they were just 20 years ago, when hub-and-spoke systems, express package delivery, just-in-time logistics, and intermodal container operations were in their infancy. Nearly all modes of transportation have experienced sharp increases in traffic volumes and changes in their methods of providing services.

[8] According to FAA statistics, 13,459 handguns and 1,151 other firearms were detected and confiscated by airport screeners from 1994 to 2000 (personal communication, FAA Office of Civil Aviation Security Operations, May 3, 2002).

It is important, therefore, to ensure that security approaches are capable of being adapted to evolving circumstances. Perhaps the best way to foster such adaptability is to mesh security with other operational tasks and objectives, such as curbing crime, dispatching and tracking vehicles, monitoring the condition of infrastructure, and ensuring safe operations.[9] Indeed, providing economic incentives for transportation users and operators to build security into their operations will be critical; simply urging greater security consciousness will not be enough, nor would it have a lasting effect in such a competitive and cost-sensitive sector.

In addition, before investing in new technologies and procedures, it is important to consider opportunities for dual use of those already at hand. The role played by FAA's air traffic controllers in grounding aircraft after the September 11 attacks, for instance, and the forensic use after the anthrax attacks of tracking codes imprinted on U.S. mail demonstrate that such dual-use opportunities exist and can be integrated into security planning. As a corollary, security-related technologies and procedures themselves can have wider utility; for example, the matching of airline passengers with their bags could also decrease the incidence of lost luggage, and closed-circuit television surveillance and undercover patrols by security personnel could reduce ordinary crimes in public places such as transit stations.[10] Such opportunities must be sought out systematically, recognizing as well that multiuse, multibenefit systems have a greater chance of being maintained and improved over time.

A security approach that capitalizes on existing processes and capabilities makes sense given the potential cost and magnitude of the security task in the evolving and expansive transportation sector. A long-term commitment to costly security technologies developed and deployed outside a systems context—such as requirements for rapid deployment of expensive and potentially immature technologies for detecting explosives—poses the risk of early and prolonged obsolescence as technologies, transportation operations, and secu-

[9] A recent NRC report (NRC 1999b) emphasizes the importance of capitalizing on other transportation system goals and features to provide security.

[10] As another example of collateral benefits, when London Transport instituted counterterrorism measures on its rail transit system, crime and vandalism fell throughout the system even as crime rates increased citywide (Jenkins 2001).

rity threats change. A more efficient, adaptable, and system-oriented approach might encompass such tactics as the randomization of security screening, the setting of traps, and the masking of detection capabilities—all to allocate security resources most effectively and to create layers of uncertainty that could inhibit terrorist activity through what might be called "curtains of mystery."

Moreover, to minimize costly disruptions to transportation services, it may be desirable to narrow the security task to the highest-risk actors and activities. To do so would require a better understanding of normal patterns of behavior and activity, allowing for the preidentification of legitimate and low-risk travelers and shippers that could be filtered out so that more security resources could be devoted to scrutinizing anomalies. To this end, for example, information gleaned from computerized airline reservation systems could be integrated with passenger and baggage screening procedures, instead of the two being treated as discrete and unconnected processes.[11] Information from ticketing that suggested an air traveler posed a risk could be conveyed to personnel at all security checkpoints, including guards at the entries to secure concourses, baggage screeners, and airline gate attendants who examine and collect boarding passes.[12] In more open transportation systems, where it can be difficult to identify and track high-risk traffic, information and communication tools could offer a means to create a virtual closed system. Large trucks, for instance, could be required to have an identifier tag affixed to the windshield and scanned at critical points along the highway. The tracking information could be used to ensure that higher-risk trucks—that is, those without tag identifiers or with unusual routings—were scrutinized more carefully at border crossings, tunnels, and major bridges down the road. As an added layer of deterrence and protection, all trucks could be subjected to random checks of the validity of the tag, as well as the legality of the driver, vehicle, and cargo.

Perhaps the most open of all transportation systems are the public transit systems of large urban areas. Indeed, transit systems around the world have

[11] The need for such integration of security capabilities was observed earlier by the White House Commission on Aviation Safety and Security (1997).

[12] This information could also be used to process individuals through all other exits from the secure area.

become recurrent terrorist targets because of their openness and concentrations of people, and the potential for attacks to cause mass disruption and alarm. Many opportunities exist for using information generated by operations (e.g., ticket reservation records, shipment manifests, passenger identification) to devise layered security systems in air and maritime transportation. Similar information is not available for many of the land transportation modes, such as public transit, whose users are often anonymous. Nevertheless, security in these other surface modes can be layered through other means while also capitalizing on dual-use applications.[13] When certain opportunities arise, such as during the design of new stations or the remodeling of existing ones, many cost-effective protective features can be added, such as good lighting, blast-resistant structures, emergency evacuation routes, and open spaces that provide broad fields of vision. And certainly in areas where free access is not required, such as at railcar and bus storage yards, fences, police patrols, and other perimeter protections can be added—not only to provide security against terrorist attacks, but also to help prevent vandalism and other crimes. The well-placed application of certain technologies, such as surveillance cameras and sensors that detect chemical and biological agents, can further strengthen the overall security system by adding an element of deterrence, as well as an early diagnosis and response capability. As they mature, moreover, facial-recognition technologies may have strategic application in some public transportation settings, thereby strengthening deterrence and detection capabilities.

If such measures are to be effective in such a ubiquitous and expansive mode of public transportation, however, security must be approached holistically. Explicit consideration must be given, for instance, to the important security function of civilian staff, such as bus and train operators and station attendants. Their visible presence alone can serve as a deterrent, and these individuals are in the best position to recognize and report situations that are out of the ordinary before they become full-blown incidents. Attention must be given to making on-site staff more visible and training them in how to react and respond appropriately—a critical responsibility, since transit operators and attendants are most likely to be the first personnel at the scene of an attack.

[13] For a more complete description of ways of layering security in public transportation, see Jenkins (2001).

Similarly, riders themselves can be an important resource. Active public cooperation and vigilance can be encouraged through such means as recurrent messages and public announcements to be alert for and report unattended articles. Indeed, it is the most crowded locations, where terrorists are most likely to strike, in which chances are greatest that a passer-by, if prompted to be attentive, will quickly notice a suspect package and alert authorities.[14]

All of these elements together—from blast-resistant designs and well-lit spaces to strategic placement of guards and fences and deliberate means of enhancing situational awareness by personnel and passengers—can provide a multitiered security system that both deters and protects. Of course, these elements must be backed up by well-devised and well-rehearsed plans for incident response and restoration of service. Transit systems that are prepared for response and recovery are less desirable targets for attackers banking on mass confusion and disorder to amplify the harm caused.[15]

## Broad-Based, Unconventional Thinking on Threats and Responses

Given the size, scope, and ubiquity of the transportation sector, coupled with its myriad owners, operators, and users, numerous opportunities exist for terrorists to exploit components of transport systems in many different, and novel, ways. After all, terrorists may not view individual transportation assets, infrastructure, and services in isolation and in traditional function-oriented ways, but as tools that can be exploited for other objectives—much as jet airliners and mailed letters were used in the fall of 2001 as weapon delivery systems. Similarly, terrorists may view components of other systems, such as the electric power grid, as a means of disrupting or impairing critical transportation services. Indeed, even the perpetrators of an attack probably could not anticipate the full array of economic and societal consequences that could arise as the resulting wave of disruption moved through many complex and interrelated systems.

Given the broad spectrum of potential opportunities for a terrorist attack, the institutions traditionally responsible for securing transportation systems

[14] See Jenkins (2001, 16–17).

[15] For a synthesis of efforts by U.S. public transportation authorities to plan for terrorist attacks, see Boyd and Sullivan (1997).

are unprepared to counter the unprecedented means by which those systems could be exploited for terrorist purposes. Yet it is critical that such possibilities and their risks be anticipated and understood if precautions are to be taken and countermeasures devised. Effective security planning and preparation require a continuous means of engaging in unbiased and nontraditional thinking about vulnerabilities and threats, their consequences, and appropriate planning and policy responses. This needed analytic capability—from scenario-based threat assessments and red teaming to systems modeling—does not exist today.

# REFERENCES

## ABBREVIATION

NRC National Research Council

Boyd, A., and J. P. Sullivan. 1997. *TCRP Synthesis of Transit Practice 27: Emergency Preparedness for Transit Terrorism*. Transportation Research Board, National Research Council, Washington, D.C.

Bureau of Transportation Statistics. 2000. *National Transportation Statistics 2000*. U.S. Department of Transportation, Washington, D.C.

Flynn, S. E. 2000a. Beyond Border Control. *Foreign Affairs*, Vol. 70, No. 6, Nov.–Dec.

Flynn, S. E. 2000b. Transportation Security: Agenda for the 21st Century. *TR News*, No. 211, Nov.–Dec., pp. 3–7.

Flynn, S. E. 2001. Bolstering the Maritime Weak Link. Testimony before the Committee on Governmental Affairs, U.S. Senate, Washington, D.C., Dec. 6.

Jenkins, B. M. 2001. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*. Report MTI-01-14. Norman Y. Mineta International Institute for Surface Transportation Policy Studies, San Jose State University, San Jose, Calif.

Leeper, J. H. 1991. Border Interdiction: The Key to National Security. Presented at 7th Annual Joint Government–Industry Symposium and Exhibition on Security Technology, Norfolk, Va., June 12.

NRC. 1999a. *Assessment of Technologies Deployed to Improve Aviation Security: First Report*. National Academy Press, Washington, D.C.

NRC. 1999b. *Improving Surface Transportation Security: A Research and Development Strategy*. National Academy Press, Washington, D.C.

White House Commission on Aviation Safety and Security. 1997. Final Report to President Clinton. Executive Office of the President, Washington, D.C., Feb. 12.

# 3

# Examples of Key Research and Technology Needs

In response to the events of September 11, scientists, engineers, and technologists in the public and private sectors alike are expending a great deal of effort on finding ways to use science and technology to counter terrorism. A strategy that can help guide those efforts to achieve maximum benefits is crucial. An essential step in devising such a strategy is to systematically identify the most important research and technology needs. The list of such needs in Box 3-1, provided as a starting point that is by no means exhaustive, shows that a great deal of research and development over a wide range of technical areas is needed in the interest of transportation security. In the following sections, these needs are reviewed in greater detail.

## Systems-Level Research

Many technological capabilities, new or enhanced, will be needed to support well-designed, layered security systems in the transportation sector. Success will not occur, however, without systems-level research to help establish the big picture within which individual efforts—some of them novel ideas and innovations, others adaptations of technologies and procedures developed elsewhere with different primary aims—each must play their separate but interconnected parts.

A fundamental need is a more thorough understanding of the operations, institutions, and other functions and characteristics of the transportation and logistics enterprises. This level of understanding is necessary to identify candidate security systems—for instance, to determine where the megaport-like

**BOX 3-1**

# KEY RESEARCH AND TECHNOLOGY NEEDS FOR TRANSPORTATION SECURITY

## SYSTEM RESEARCH

### OPERATIONS

- Understanding of normal patterns of transportation activity and behavior
- Identification of anomalous and suspect activities
- Dual-use opportunities
- Opportunities to leverage security in operations

### HUMAN FACTORS

- Ability of security personnel to recognize context and patterns
- Design of security devices, facilities, and procedures that are efficient and reliable
- Understanding of means of obscuring the risk of getting caught
- Understanding of how technology can complement and supplement humans
- Creation of security institutions that are performance driven

### LEGAL AND ETHICAL ISSUES

- Acceptability of surveillance systems
- Use of biometrics for identify verification
- Use of prescreening systems, and means to collect and protect personal information

## DETERRENCE

- Psychological studies to model terrorist types
- Deterrent effects of tactics to create uncertainty (e.g., "curtains of mystery")
- Deterrent effects of layered countermeasures

### PREVENTION

- Data-mining and other data evaluation techniques to filter out lower-risk users
- Understanding of the markers of risk associated with travelers
- Explosive detection systems capable of detecting a wider range of materials
- Means to network and combine sensors
- Standoff and accurate field sensors with low rates of false alarm
- Biometrics and other means of verifying travelers and operators

### MONITORING AND MITIGATION

- Real-time chemical sensors that are effective in complex environments
- Construction methods to harden transportation facilities
- Dispersal models for various agents in transportation environments
- Ways to use dispatch and control systems for consequence management
- Means of protecting traffic control systems from physical and cyber attacks

### RESPONSE AND RECOVERY

- Neutralizing agents, and robots that can be used to test areas and perform decontamination
- Communications capacity for emergency responders
- Regional emergency-response plans that coordinate highways and public transit

### INVESTIGATION AND ATTRIBUTION

- Integration of investigative capabilities into transportation operations and control systems.

linchpins (see Box 2-1) may lie for new security approaches. Systems-level research and analysis would also provide an understanding of normal patterns of transportation activity and behavior. Such understanding is essential for developing security programs that can filter out trusted passengers and shippers, and for designing and deploying networks of sensors in ways that enhance accuracy and reduce the incidence of missed and false alarms. An understanding of the operations and economics of transportation systems is also crucial if security is to be integrated with other transportation system objectives (as discussed in Chapter 2). For example, shippers and other commercial users of transportation may be willing to accept the outlays required for blast-resistant containers, electronic tamper-proof seals, and real-time recording of shipment manifests if those measures facilitate the general movement of cargo and better secure it against theft and loss.[1]

It will also be important to recognize that certain security approaches are practical and acceptable under some circumstances and impractical and unacceptable under others. For example, in the wake of the September 11 attacks, airline passengers have demonstrated a willingness to endure more time-consuming and intrusive security procedures. For many travelers, airline trips are long in any case and not a daily occurrence, and extra time can thus be spared for additional security measures. To be sure, similar inconveniences would not be so well accepted by passengers in the more time-sensitive modes used for daily commuting, and air travelers' impatience with burdensome security procedures can be expected to grow over time, especially if the public views security procedures as more symbolic than substantive.

The development of effective security measures therefore depends not only on good research pertaining to transportation operations, but also on an understanding of human factors. Such insight is needed for everything from designing airport security checkpoints that are more efficient and less error-prone to developing means of deterring terrorists through the "curtains of mystery" discussed in Chapter 2. Indeed, human factors are integral to all security initiatives, whether they entail technologies, procedures, or organizational structures.

[1] See Badolato (2000) and Flynn (2000a; 2000b).

It is especially important that the role of people in operations and security be determined not by default, simply on the basis of technological possibilities, but as a result of systematic evaluations of human strengths and weaknesses that can be complemented and supplemented by technology. Human strengths, such as sensitivity to context and pattern recognition, may be difficult or unnecessary to replicate. Indeed, it may turn out that some technologies do not hold promise because they are inferior to, or incompatible with, the performance of human users; for instance, they might interfere with the performance of flight crews, bus drivers, or screeners.[2]

Many other nontechnical issues also loom large in the development and deployment of effective security systems. Privacy and civil rights controversies, for example, dominate the debate over data-mining and biometric technologies for passenger prescreening, identification, and surveillance—a debate pertinent not only to the transportation sector, but also to other technology-based realms.[3] Though technological advances will undoubtedly continue to offer many new capabilities, some will raise new legal and ethical issues that must be addressed long before those capabilities are used. Sound systems-level research and analyses—addressing operational, institutional, and societal dimensions—can bring these issues to light.

To be sure, the restructuring of transportation security technologies, techniques, and procedures to form coherent systems will not be easy. It will require an ability and willingness to step back and define security goals and performance expectations; to identify the layered systems best suited to meeting those goals and expectations; and to work with many public, private, and foreign entities to implement those systems. Security planners must be willing to question many existing security rules, institutional relationships, tactics, and technologies. To this end, much strategic planning, supported by well-targeted, systems-level research and analysis, will be required.

---

[2] Prior experience with new technologies in aviation has shown the value of this approach, and FAA is now committed to early integration of human factors in its acquisition programs.

[3] As an example, civil rights issues associated with automated passenger-profiling systems are discussed by the White House Commission on Aviation Safety and Security (1997), which also offers recommendations for addressing those issues. In addition, the Computer Science and Telecommunication Board (CSTB 2002) reviews the policy and technological issues associated with national identification systems.

## DETERRENCE

As noted earlier, the impracticality of eliminating all transportation vulnerabilities means that efforts to deter must be a key part of transportation security strategies. That reality, together with the likelihood that deterrence has likely stopped many hostile acts against aircraft during the past decade, gives deterrence an essential early role in the line of defense against transportation terrorism. In a sector as large and as open as transportation, however, deterrence—or deflection of the hostile act to a less susceptible or less damaging target—cannot be achieved simply through traditional means involving "guards, guns, and gates." Instead, deterrence will require sound intelligence information related to transportation security, along with the innovative use of resources and capabilities that together can create a high degree of uncertainty among terrorists about their chances of defeating the system (again, those "curtains of mystery").

The extent to which uncertainty can deter a terrorist from a specific target is itself a potentially important avenue of inquiry. How does the fear of getting caught influence actions? Even a terrorist intent on suicide does not want to be stopped before achieving his or her goals. Researchers conducting psychological studies have sought to model criminal attitudes by interviewing perpetrators, and similar studies could presumably be directed to terrorist attitudes in an effort to better understand the factors influencing their decisions to attack or avoid targets. Such knowledge could prove useful in assessing the deterrent effects of specific tactics, such as the use of chemical-sniffing dogs, the randomized deployment of surveillance cameras, and the publicizing of new but unspecified passenger screening procedures.

## PREVENTION

If deterrence is unsuccessful, the next line of defense is prevention, whether by denying access through physical means—guards and fences, for example—or by using other methods of interception, such as passenger profiling, baggage inspection, and explosive detection. A topic likely to generate much research and debate in the years ahead is how best to filter out the lower-risk users of transportation systems so that security resources can be focused on anomalies

and higher-risk traffic. Advanced information technologies offer some promising tools for such identification and prescreening. What is needed, however, is a better understanding of the markers of risk, the kinds of data useful for identifying these markers, and the best means of interpreting and using the results for detection and control purposes.

For example, the application of automated passenger prescreening systems may depend less on advances in biometrics, artificial intelligence, statistics, and computer hardware than on the kinds and quality of data that can be employed in these systems. Not only must the multiple, heterogeneous databases involved be accurate and compatible (both of which present major challenges), but the right information must also be extracted and combined. For example, how can data on a traveler's financial records, immigration status, legal history, demographic characteristics, and matches to traveling companions on the same flight be used to evaluate his or her security risk, and who will then act on the results? Will new databases be created by the linking of various private and public data sources? And if so, how will the information be stored and protected, and who will have access to it and for what purposes? Research on numerous such issues is clearly required to help policy makers evaluate preventive measures.[4]

Yet another prevention-related need is for explosive-detection systems that are sensitive to a wider range of materials. At the moment, many threats are not detectable; for instance, a pouch sealed in plastic and taped on a person's body may not register with available screening devices. New and emerging techniques could help augment existing detection capabilities. For example, three sensor technologies for detecting explosives appear to hold promise: X-ray diffraction, which detects several types of explosives; microwave/millimeter wave scanners, which can penetrate denser substances; and nuclear quadrupole resonance, which can identify the chemical composition of selected materials.[5]

[4] See CSTB (2002) for a review of important technological and policy issues associated with the development and use of databases for identification systems.

[5] See NRC (1996; 1999; 2002) for more detailed assessments of deployed and emerging technologies designed to improve aviation security.

What is clear, however, is that no single sensor technology can be expected to detect all threats with acceptable accuracy. Thus an array of sensor technologies will need to be developed and used together in a reliable, networked manner whereby each sensor can cross-check the validity of the readings of others. Such systematic cross-checking can help reduce the incidence of false alarms and the need for inconvenient and costly follow-on searches, such as manual baggage inspections.

In general, all detectors—whether they sense explosives, say, or radiological materials—need to be made more accurate for use in transportation modes, where an excessive rate of false alarms can wreak havoc. They must also be made smaller, more affordable, and capable of operating at greater ranges. These latter requirements are particularly important if detectors are to be deployed strategically in the surface transportation modes.

## Monitoring and Mitigation

Knowing when a hostile attack is under way, diagnosing it quickly and accurately, predicting its course, and mitigating its harmful effects are crucial capabilities. Monitoring is essential to all these crisis-management functions. Indeed, as noted in Chapter 2, the use of FAA's air traffic management system to ground aircraft on September 11 demonstrated how existing traffic operation and control systems could be used to detect a terrorist attack in progress and help manage the crisis. Likewise, the fast and decisive actions taken by local traffic control centers to prevent commuter and subway trains from passing under the World Trade Center may have saved hundreds of lives.

Monitoring capabilities that are not yet available but could prove crucial in transportation settings include real-time sensors that can rapidly detect the presence of a wide variety of chemical agents. In a busy transportation environment, rapid recognition of a threat is critical to ensure appropriate response. A prerequisite for the development of such sensor systems is baseline information on the background chemicals in facilities such as subway systems and airport terminals, especially to ensure that sensor systems are designed to balance the risks associated with false positive and negative readings. On the one hand, excessive false alarm rates are a major concern for

transportation operators, lest localized service disruptions propagate regularly across an entire network; excessive false alarms eventually lead to alerts being ignored and alarm systems being turned off. On the other hand, just one missed or neglected alarm runs the risk of exposing thousands of people to deadly agents and postponing effective emergency response. An appropriate balance must be struck between such risks. To this end, risk modeling and human factors assessments are essential.

With regard to mitigation, research on architectural features, materials, and construction methods that can be used to harden transportation facilities has the potential to illuminate ways of mitigating the effects of a blast. This research could also reveal means of protecting structures from earthquakes and other natural disasters, although such correlations warrant further study. Similarly, the design of blast-resistant containers for aviation could be helpful for other modes. The Department of Defense has already conducted much research on blast-resistant designs, materials, and structures, some of which may be applicable for transportation purposes.

There is a great deal of interest in the transportation community not only in mitigating the effects of explosions, but also in containing releases of chemical and biological agents. Specialized research on the dispersal of various agents within different transportation environments is required. An understanding is needed, for instance, of how trains moving in subway tunnels may push contaminants within the underground system and through external vents into the streets above.[6] In addition to aiding in the design of sensor networks, such knowledge could help in the development of effective mitigation measures, such as ventilation barriers and filters, and in the formulation of emergency response plans.

## Response and Recovery

A key to effective response following an event is the capability to communicate and coordinate the actions of firefighters, police, elected officials, and transportation agencies across numerous jurisdictions. Communication

[6] See Policastro and Gordon (1999) and Policastro et al. (2002).

paths, equipment, and protocols must be established in advance as part of emergency response plans, and sizable capacity must be made available quickly without having to disrupt basic communication links. R&D to enhance emergency decision making and communication protocols and capabilities is important to the transportation community, as it is to other participants in incident response.

As noted earlier, the ability to recover and reconstitute transportation services quickly is crucial for limiting the cascading effects of terrorist attacks. Doing so may require a range of capabilities, from specific means to reroute traffic around disrupted areas to the development of well-rehearsed regional emergency response plans that coordinate highway and public transportation systems. The restoration of transportation services following an attack also requires a range of technological capabilities—for example, neutralizing agents and robots that can survey affected areas and perform decontamination, and tools for the rapid repair of key infrastructure elements to render them at least minimally functional.

## Investigation and Attribution

To aid in the deterrence and prevention of further attacks, technologies and techniques to assist in investigation and attribution of past attacks will be needed. Catching perpetrators before they can do harm again is, of course, one reason to investigate and seek attribution. Another is to learn from an attack in order to prevent others in the future. Following the September 11 attacks, data gathered from the air traffic control system were used to reconstruct the timing and pattern of the four airline hijackings. Much as cockpit voice recorders and flight data boxes are critical for reconstructing airline crashes, such analyses could prove helpful in designing better means of monitoring traffic and recognizing the early signs of an attack. How best to develop such investigative capabilities is a potentially important avenue of inquiry.

# REFERENCES

## ABBREVIATIONS

| | |
|---|---|
| CSTB | Computer Science and Telecommunication Board |
| NRC | National Research Council |

Badolato, E. 2000. Cargo Security: High-Tech Protection, High-Tech Threats. *TR News*, No. 211, Nov.–Dec., pp.14–17.

CSTB. 2002. *IDs—Not That Easy: Questions About National Identity Systems*. National Academy Press, Washington, D.C.

Flynn, S. E. 2000a. Beyond Border Control. *Foreign Affairs*, Vol. 70, No. 6, Nov.–Dec.

Flynn, S. E. 2000b. Transportation Security: Agenda for the 21st Century. *TR News*, No. 211, Nov.–Dec., pp. 3–7.

NRC. 1996. *Airline Passenger Security Screening: New Technologies and Implementation Issues*. Publication NMAB-482-1. National Academy Press, Washington, D.C.

NRC. 1999. *Improving Surface Transportation Security: A Research and Development Strategy*. National Academy Press, Washington, D.C.

NRC. 2002. *Assessment of Technologies Deployed to Improve Aviation Security: Second Report. Progress Toward Objectives*. National Academy Press, Washington, D.C.

Policastro, A. J., and S. P. Gordon. 1999. The Use of Technology in Preparing Subway Systems for Chemical/Biological Terrorism. Proceedings of the 1999 Commuter Rail/Rapid Transit Conference, Toronto, American Public Transportation Association.

Policastro, A. J., F. O'Hare, D. Brown, M. Lazaro, and S. Filer. 2002. *Guidelines for Managing Suspected Chemical and Biological Agent Incidents in Rail Tunnel System*. Federal Transit Administration, U.S. Department of Transportation, Washington, D.C., Jan.

White House Commission on Aviation Safety and Security. 1997. Final Report to President Clinton. Executive Office of the President, Washington, D.C., Feb. 12.

# 4

# Advice to TSA on Strategic Research and Planning

The Aviation and Transportation Security Act of 2001, which created TSA, set forth a series of responsibilities and deadlines for the agency, from the assumption of airline passenger and baggage screening functions to the deployment of air marshals and explosive-detection systems at commercial airports. Whereas most of the act's provisions deal exclusively with civil aviation, TSA is also assigned a broader security mandate—affecting all transport modes—that includes the following statutory responsibilities:

- Receive, assess, and distribute intelligence information related to transportation security;
- Assess threats to transportation;
- Develop policies, strategies, and plans for dealing with threats to transportation security;
- Make other plans related to transportation security, including coordination of countermeasures with appropriate departments and agencies;
- Serve as the primary liaison for transportation security to the intelligence and law enforcement communities;
- Enforce security-related regulations and requirements;
- Inspect, maintain, and test security facilities, equipment, and systems;
- Ensure the adequacy of security measures for the transportation of cargo; and
- Identify and undertake R&D activities necessary to enhance transportation security.

The many new and challenging aviation-related operational and implementation requirements set forth in the act are understandably consuming much

of TSA's financial and organizational resources, and they are likely to continue to do so for some time. Nevertheless, the overarching mission responsibilities listed above are essential to the agency's success and cannot remain neglected for long. The following three recommendations for assuming this strategic role are offered to DOT and TSA. The first stems from a recognition that the transportation sector is so large, dynamic, and fragmented that no single agency can be responsible for day-to-day security tactics and technologies. If TSA is to have a meaningful role in securing all modes of transportation, it must be prepared to offer advice and assistance at a strategic level. The second and third recommendations reflect the fact that TSA is the only national entity with responsibility for security in the transportation sector as a whole. The agency is therefore in the best position to ensure that research is undertaken that is useful to all transportation modes, and that good information on security technologies and methods is provided to the many public- and private-sector users and providers of transportation services.

## Creating a Strategic Research and Planning Capacity

***TSA should establish a strategic research and planning office—attuned to, but distinct from, the agency's operational and enforcement responsibilities—that will work with DOT, the modal agencies, other federal agencies, state and local governments, and other elements of the public and private sectors on security system research, planning, and deployment.***

Having a strong analytic capability to undertake systems planning and risk assessment, this office could

- Devise and evaluate alternative security system concepts for the different modes of transportation through collaboration with public- and private-sector owners, operators, and users, and through the application of operations research and human factors expertise;
- Ensure that gaps do not exist in security planning and preparation because of the narrow purview, perspectives, and knowledge of individual modal agencies and owners, operators, and users of transportation systems;

- Encourage the explicit inclusion of security goals in the transportation planning process and in the design of vehicles, facilities, and operating systems by seeking out dual-use opportunities, and by identifying design standards for new transportation systems and facilities that fully integrate security considerations;
- Advise metropolitan governments and transportation agencies on the need to develop integrated regional emergency response plans; and advise local and state transportation agencies, public transit authorities, and related entities on how to reshape their administrative structures so as to give security prominence in their planning and decision making;
- Explore ways in which security enhancements can be encouraged, and market-related and institutional barriers to the deployment of security measures can be overcome—for example, through balanced roles for regulation, subsidy, education, and standards setting;
- Work with other countries and international standards-setting bodies to exchange information about international shipments, coordinate security measures and overall system strategies, and collaborate in R&D activities; and
- Develop a critical research agenda in support of transportation security systems.

Multimodal in its orientation, such a strategic office would require systems planning and engineering expertise and the capability to conduct risk assessments. To this end, TSA could make effective use of DOT's Volpe National Transportation Systems Center and other resources that TSA and Volpe could bring to bear. The recommended office would also need to interact closely with other federal agencies (such as the Coast Guard, Customs Service, Federal Emergency Management Agency, and Immigration and Naturalization Service) in domains of responsibility integral to transportation; with international standards-setting bodies (such as the International Civil Aviation Organization, World Customs Organization, and International Maritime Organization); and with state and local agencies at the implementation level. To be effective and trusted, TSA must be more than a regulatory and enforcement arm of DOT; it must find ways to share needed expertise and information and to work constructively with those parties—from modal agencies to public- and private-sector transportation system operators—entrusted with

fielding security solutions. A strategic research and planning office within TSA, unencumbered by rulemaking, enforcement, and operational responsibilities, could offer these needed services.

## Marshaling R&D in Support of Transportation Security

A number of important systems analysis and technology needs for transportation security are identified in this report, and TSA is uniquely positioned to undertake, encourage, and guide much of the R&D that can meet these needs. To help devise coherent security systems and to procure and recommend supporting technologies, TSA must have its own analysis and research capacity. But it also must have the ability to draw on the rich and varied R&D capabilities within the transportation sector, as well as those of the federal government and the science and technology community at large.

The modal agencies within DOT, as well as other federal agencies with responsibility for security functions related to transportation (such as the Customs Service and the Immigration and Naturalization Service), have missions ranging from safety assurance to revenue collection and drug interdiction. Most have small R&D budgets to support these missions; hence, these agencies can be expected to seek a maximum return on their R&D investments by sponsoring research that meets their own mission-oriented needs first, while offering security advantages as an added benefit. As discussed in Chapter 2, such duality of purpose can be beneficial, but approaching security as a side benefit could result in research gaps and a tendency to neglect comprehensive, systems-level research.

In viewing the R&D activities of the modal agencies in their totality and from a broader systems perspective, TSA could help fill these research gaps by offering agencies guidance on the allocation of their R&D investments. From this vantage point, TSA could monitor progress on security-related R&D, observe where modest additional investments might yield large benefits, and orchestrate ways to encourage such investments.

To be sure, much of the R&D that will be needed must take place outside the transportation realm—in the nation's universities and research institutions and with the support of much larger R&D sponsors, such as the

Department of Defense, the National Institutes of Health, and the National Science Foundation. By making the needs and parameters of transportation security systems more widely known, however, TSA could tap this research from outside the transportation field and help identify and shape those R&D efforts most relevant to transportation applications.

***TSA should collaborate with the public and private sectors to build a strong foundation of research on human factors and transportation operations, and to make the evaluation of security system concepts a central element of its collaborative research program. TSA should establish an in-house research capacity to undertake such concept evaluations and to support its own large security operations and technology acquisition programs. At the same time, the agency should adopt a broader, architect-like role in promoting and marshaling R&D to advance these security systems, especially by tapping into the security-related R&D of other government agencies, the broader transportation community, universities, research institutions, and the private sector.***

## A Technology Guidance and Evaluation Capacity

Academia and the private sector are eager to contribute creative ideas and technologies to the task of enhancing transportation security. At the same time, transportation system owners and operators want to hear their advice and apply the results of good research and technology development. Currently, however, many of the ideas and technologies being proposed for security purposes have only limited potential for application—not only because of inadequate incentives to invest in them, but also because technologies and techniques that appear promising in isolation do not fit well in a security system or are incompatible with the transportation operating environment.

TSA has a potential catalytic role here in providing scientists and technologists with clearer targets for their research and innovation efforts. In conjunction with commercial developers and transportation system owners and users, TSA could help develop product evaluation standards and methods, sponsor prototype demonstrations, and conduct field trials. Precedents for

such clearinghouse and evaluation services can be found in the transportation sector and elsewhere, and they could be useful as models.[1]

***TSA should create a technology guidance, evaluation, and clearinghouse capacity to provide developers with performance goals for their products, and to advise transportation system operators on security-related technologies that are available or under development.***

[1] An example is the Highway Innovation Technology Evaluation Center, created with seed money from the Federal Highway Administration and managed by the Civil Engineering Research Foundation of the American Society of Civil Engineers.

# 5

# Concluding Observations

The nascent Transportation Security Administration provides a new, and rare, opportunity to approach transportation security in a strategic manner based on the application of sound science and technology. It is essential that this opportunity not be lost. DOT, and TSA in particular, should take steps now to build this strategic capability and ensure its permanence. In a similar manner, others have urged the Office of Homeland Security to adopt such a strategic and architect-like role on a broader scale for the federal government as a whole (Carter 2002).

TSA's security mission does not extend beyond the transportation sector. As the events of September 11 revealed, however, vulnerabilities to terrorist acts may not be limited to components within particular transportation modes and systems. In fact, such vulnerabilities may exist in the interactions among modes or between transportation and other domains, such as energy and computer systems. Hence, it is essential that the vulnerabilities existing at these intersections, the threats that may be associated with them, and appropriate strategies for response be addressed. A broad-based understanding of terrorist threats is needed to inform the transportation community and others on the front lines of defense as they formulate security plans and take precautions.

An entity outside the normal organizational setting—unencumbered by operational, oversight, and regulatory responsibilities—is needed to provide this capability. The mission of this entity would be to explore and systematically assess the broad spectrum of vulnerabilities to terrorist attacks, probable responses to such attacks, and ensuing consequences. By involving and informing TSA and the transportation community, as well as parties in other

domains, the work of this analytic entity could provide valuable guidance to transportation owners, operators, and overseers as they prioritize and make security preparations. The National Academies report *Making the Nation Safer* urges the creation of a Homeland Security Institute to provide this essential analytic and response capacity (see the appendix to the present report).

## Reference

Carter, A. B. 2002. The Architecture of Government in the Face of Terrorism. *International Security,* Vol. 26, No. 3, pp. 5–23.

# Appendix
# Making the Nation Safer[1]

## Executive Summary

*In the war against terrorism, America's vast science and technology base provides us with a key advantage.*

—President George W. Bush, June 6, 2002[2]

## Context and Contents of the Report

Terrorism is a serious threat to the security of the United States and indeed the world. The vulnerability of societies to terrorist attacks results in part from the proliferation of chemical, biological, and nuclear weapons of mass destruction, but it also is a consequence of the highly efficient and interconnected systems that we rely on for key services such as transportation, information, energy, and health care. The efficient functioning of these systems reflects great technological achievements of the past century, but interconnectedness within and across systems also means that infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures. As terrorists seek to exploit these vulnerabilities, it is fitting that we

[1] *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, prepublication copy from June 25, 2002. National Research Council, National Academy Press.

[2] From the President's June 6, 2002, address to the nation. The text of this speech is available online at http://www.whitehouse.gov/news/releases/2002/06/20020606-8.html.

harness the nation's exceptional scientific and technological capabilities to counter terrorist threats.

This report describes many ways in which science and engineering can contribute to making the nation safer against the threat of catastrophic terrorism. The report identifies key actions that can be undertaken now, based on knowledge and technologies in hand, and, equally importantly describes key opportunities for reducing current and future risks even further through longer-term research and development activities. However, science and technology are but one element in a broad array of potential approaches to reducing the threat of terrorism. Diplomacy, international relations, military actions, intelligence gathering, and other instruments of national policy well beyond the scope of this study all have critical roles to play.

Our society is too complex and interconnected to defend against all possible threats. As some threats are diminished others may arise; terrorists may change their goals and tactics. While this report describes what in the committee's best judgment are the top-priority actions and research objectives for harnessing science and technology to meet today's threats, the most important conclusion of this report is that the nation needs a well-organized and disciplined ability to respond as circumstances change. In that sense this is not an enduring plan for technical work, but rather a starting point from which the nation can create defenses-in-depth against the new threat. For that reason it is especially important that strengthening the national effort in long-term research that can create new solutions be a cornerstone of the strategy for countering terrorism.

## Top-Priority Technical Recommendations

Key elements or infrastructures of society can be means of attack, targets, and means of response. While some systems and technologies can be classified roughly in one or another of these categories (i.e., nuclear weapons are primarily means of attack; energy systems are primarily targets), most systems and technologies can fit into multiple categories. For example, air transportation is both a target and a means of attack, and information and telecommunications systems are both targets and means of response. The committee considered

nine areas, each of which is discussed in a separate chapter. The areas are nuclear and radiological threats, human and agricultural health systems, toxic chemicals and explosive materials, information technology, energy systems, transportation systems, cities and fixed infrastructure, the response of people to terrorism, and complex and interdependent systems.

The chapters on these nine areas each contain a number of recommendations, all describing what the committee believes are critical ways to make the nation safer from terrorism. The actions and research opportunities described in the chapters cover a wide assortment of approaches, fields, and systems; they range from immediate applications of existing technology to development and deployment efforts to long-term basic research programs. Based on an understanding of the difficulty of launching particular kinds of attacks and the feasibility of limiting the damage and recovering from such attacks, the committee was able to prioritize within each area in order to determine the topics covered later in this executive summary, where the committee's top-priority concepts and actions in each area are described. To *definitively* determine the most important actions within and across all nine areas would require knowledge of the relative likelihood of threats and information about the intent and capability of terrorists. However, based on information in prior major studies and commission reports about the current threat, the committee provides a short list of important technical initiatives that span the areas (see Box ES-1). This list includes seven ways to immediately apply existing knowledge and technology to make the nation safer and seven areas of research and development in which it is urgent that programs be initiated or strengthened. These initiatives illustrate the types of actions recommended by the committee throughout this report.

## General Principles and Strategies for How Science and Technology Can Help Protect the Nation

In this report, the committee provides a broad range of recommendations designed to demonstrate how science and engineering can contribute to counterterrorism efforts. The suggested actions include support for all phases of countering terrorist threats—intelligence and surveillance, prevention, pro-

**Box ES-1**

## Fourteen of the Most Important Technical Initiatives

### Immediate Applications of Existing Technologies

1. Develop and utilize robust systems for protection, control, and accounting of nuclear weapons and special nuclear materials at their sources.

2. Ensure production and distribution of known treatments and preventatives for pathogens.

3. Design, test, and install coherent layered security systems for all transportation modes, particularly shipping containers and vehicles that contain large quantities of toxic or flammable materials.

4. Protect energy distribution services by improving security for supervisory control and data acquisition (SCADA) systems and providing physical protection for key elements of the electric-power grid.

5. Reduce the vulnerability and improve the effectiveness of air filtration in ventilation systems.

6. Deploy known technologies and standards for allowing emergency responders to reliably communicate with each other.

7. Ensure that trusted spokespersons will be able to inform the public promptly and with technical authority whenever the technical aspects of an emergency are dominant in the public's concerns.

*(continued)*

**Box ES-1** *(continued)* **FOURTEEN OF THE MOST IMPORTANT TECHNICAL INITIATIVES**

## URGENT RESEARCH OPPORTUNITIES

1. Develop effective treatments and preventatives for known pathogens for which current responses are unavailable and for potential emerging pathogens.

2. Develop, test, and implement an intelligent, adaptive electric-power grid.

3. Advance the practical utility of data fusion and data mining for intelligence analysis, and enhance information security against cyberattacks.

4. Develop new and better technologies (e.g., protective gear, sensors, communications) for emergency responders.

5. Advance engineering design technologies and fire-rating standards for blast- and fire-resistant buildings.

6. Develop sensor and surveillance systems (for a wide range of targets) that create useful information for emergency officials and decision makers.

7. Develop new methods and standards for filtering air against both chemicals and pathogens as well as better methods and standards for decontamination.

tection, interdiction, response and recovery, and attribution—as well as ways to improve our ability to perform analysis and invent new technologies. Different phases have varying importance in each of the nine areas examined in the report. For example, the nuclear threat must be addressed at the earliest stages, when intelligence and surveillance based on international cooperation are critical for preventing the manufacture and use of nuclear weapons by terrorists. For biological threats, the situation is reversed: An attack is relatively easy to initiate and hard to prevent, but there are many opportunities for technological intervention to mitigate the effects. In other cases, such as an attack on the electrical power system, it is possible both to make the attack more difficult and to ameliorate its effects after it has been initiated.

Despite such fundamental differences in the approaches needed for countering different classes of terrorist threats, some general principles and strategies underlie recommendations presented in all of the areas:

- Identify and repair the weakest links in vulnerable systems and infrastructures.
- Use defenses-in-depth (do not rely only on perimeter defenses or firewalls).
- Use "circuit breakers" to isolate and stabilize failing system elements.
- Build security into basic system designs where possible.
- Build flexibility into systems so that they can be modified to address unforeseen threats.
- Search for technologies that reduce costs or provide ancillary benefits to civil society to ensure a sustainable effort against terrorist threats.

Following is a synthesis of the key findings and recommendations in each of the nine areas examined by the committee.

## Nuclear and Radiological Threats

Science and technology are essential ingredients of a multilayered systems approach for defending the United States against terrorist attacks involving stolen nuclear weapons, improvised nuclear devices, and radiological dispersion devices. The first line of homeland defense is robust systems for the protection, control, and accounting of nuclear weapons and special nuclear material at their

sources. The United States has made a good start on deploying such systems in Russia, which possesses large stockpiles of weapons and special nuclear material, but cooperative efforts must be pursued with new urgency. **The United States should accelerate its bilateral materials protection, control, and accounting program in Russia to safeguard small nuclear warheads and special nuclear materials, particularly highly enriched uranium. The United States also should increase the priority and pace of cooperative efforts with Russia to safeguard its highly enriched uranium by blending down this material to an intermediate enrichment of less than 20 percent U-235 as soon as possible.**

Systems to detect the movement of illicit weapons and materials could be most effectively deployed at a limited number of strategic transportation "choke points" such as critical border transit points in countries like Russia, major global cargo-container ports, major U.S. airports, and major pinch points in the U.S. interstate highway system. **A focused and coordinated near-term effort should be made to evaluate and improve the efficacy of special nuclear material detection systems that could be deployed at strategic choke points for homeland defense. R&D support also should be provided for improving the technological capabilities of special nuclear material detection systems, especially for detecting highly enriched uranium.**

Responses to nuclear and radiological attacks fall into two distinct categories that could require very different types of governmental actions: attacks involving the detonation of a nuclear weapon or improvised nuclear device, and attacks involving radiological dispersion devices. Planning has been minimal at the federal or local levels for responding to either class of attack. **Immediate steps should be taken to update the Federal Radiological Emergency Response Plan, or to develop a separate plan, to respond to nuclear and radiological terrorist attacks, especially an attack with a nuclear weapon on a U.S. city.**

As the history of the Cold War has shown, the most effective defense against attacks with nuclear weapons is a policy of nuclear retaliation, but retaliation requires that the perpetrator of an attack be definitively identified. The technology for developing the needed attribution capability exists but has to be assembled, an effort that is now under way by the Defense Threat Reduction Agency but is expected to take several years to complete. **Given the potential importance of attribution to deterring nuclear attacks, the**

**Defense Threat Reduction Agency's efforts to develop an attribution capability should continue to declared operability as quickly as practical.**

Physical and operational changes may have to be made to some of the nation's nuclear power plants to mitigate vulnerabilities to attacks from the air with a large commercial airliner or a smaller aircraft loaded with high explosives, and possibly attacks from the ground using high-explosive projectiles. The technical analyses that are now being carried out by the U.S. Nuclear Regulatory Commission and industry to understand the effects of such attacks on reactor containment buildings and essential auxiliary facilities are critical to understanding the full magnitude of this threat. **These analyses should be carried to completion as soon as possible, and follow-on work to identify vulnerabilities on a plant-by-plant basis should be undertaken as soon as these initial studies are completed.**

The likely aim of a terrorist attack with a radiological dispersion device would be to spread fear and panic and cause disruption. Recovery from an attack would therefore depend on how the attack is handled by first responders, political leaders, the media, and general members of the public. **A technically credible spokesperson at the national level who is perceived as being outside the political arena should be prepared to provide accurate and usable information to the media and public concerning public health and safety risks and appropriate response actions in the aftermath of a nuclear or radiological attack.**

Although radiological attacks would be unlikely to cause large numbers of casualties, the potential for inflicting economic loss and causing terror or panic warrants increased attention to the control and use of radiological sources by regulatory agencies and materials licensees. **The U.S. Nuclear Regulatory Commission and states with agreements with this agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks, as well as requirements for securing and tracking these sources.**

Important progress is being made by the R&D and policy communities on reducing the nation's vulnerability to nuclear and radiological terrorism. There is not much evidence, however, that the R&D activities are being coordinated, that thought is being given to prioritizing these activities against

other national counterterrorism needs, or that effective mechanisms are in place to transfer the results of these activities to applications. **A single federal agency should be designated as the nation's lead research and development agency for nuclear and radiological counterterrorism.** This agency should develop a focused and adequately funded research and development program and should work to ensure that effective mechanisms are in place for the timely transfer of results to the homeland defense effort.

## Human and Agricultural Health Systems

Just a few individuals with specialized scientific skills and access to a laboratory could inexpensively and easily produce a panoply of lethal biological weapons that might seriously threaten the U.S. population. Moreover, they could manufacture such biological agents with commercially available equipment—that is, equipment that could also be used to make chemicals, pharmaceuticals, foods, or beer—and therefore remain inconspicuous.

The attacks of September 11 and the release of anthrax spores revealed enormous vulnerabilities in the U.S. public-health infrastructure and suggested similar vulnerabilities in the agricultural infrastructure as well. The traditional public health response—surveillance (intelligence), prevention, detection, response, recovery, and attribution—is the paradigm for the national response not only to all forms of terrorism but also to emerging infectious diseases. Thus, investments in research on bioterrorism will have enormous potential for application in the detection, prevention, and treatment of emerging infectious diseases that also are unpredictable and against which we must be prepared.

The deciphering of the human genome sequence and the complete elucidation of numerous pathogen genomes, rapidly increasing understanding of the molecular mechanisms of pathogenesis and of immune responses, and new strategies for designing drugs and vaccines all offer unprecedented opportunities to use science to counter bioterrorist threats. But these same developments also allow science to be misused to create new agents of mass destruction. Hence the effort to confront bioterrorism must be a global one.

**First, new tools for the surveillance, detection, and diagnosis of bioterrorist threat agents should be developed.** Knowledge of the genome sequences of major pathogens allows new molecular technologies to be developed for the sensitive detection of pathogens. These technologies offer enormous possibilities for surveillance of infectious agents in our environment, the identification of pathogens, and rapid and accurate diagnoses. For these new technologies to be used effectively to provide early warnings, there is a need to link information from the doctor's office or the hospital's emergency room to city and state departments of health, thereby enabling detection of an outbreak and a rational and effective response. These capabilities will be important both for responding to attacks on agricultural systems (animals and crops) and for protecting humans, and they will require careful evaluation and standards. There is an urgent need for an integrated system to protect our food supply from the farm to the dinner table.

**To be able to respond to current and future biological threats, we will need to greatly expand research programs aimed at increasing our knowledge of the pathogenesis of and immune responses to biological infectious agents.** The recent anthrax attacks revealed how little is known about many potential biological threats in terms of dose, mechanisms of disease production, drug targets, and requirements for immunity. It is clear that development of therapeutics and vaccines will require more research on pathogenesis and protective host responses, but financial incentives, indemnification, and regulatory changes may be needed to allow the pharmaceutical industry to pursue such efforts. **Because markets are very limited for vaccines and drugs for countering potential bioterrorist agents, special institutes may have to be established for carrying out biohazardous research and producing drugs and vaccines. The Department of Health and Human Services and the Food and Drug Administration (FDA) should investigate strategies—including the modification of regulatory procedures—to encourage the development of new drugs, vaccines, and devices to address bioterrorist threats.**

**Research efforts critical to deterrence, response, and recovery—particularly decontamination and bioterrorism forensics—should be strengthened. Appropriate scientific expertise should be integrated into the government agencies with principal responsibilities for emergency response and post-event investigations.** Modeling tools for analyzing the health and economic

impacts of bioterrorist attacks are needed in order to anticipate and prepare for these threats. Techniques for protection of individuals and buildings should be developed, together with methods of decontamination in the event that such defenses are breached. In addition, multidisciplinary research in bioterrorism forensics is necessary to enable attribution of a weapon to its source and the identification of persons involved in a bioterrorist act.

Preparedness for bioterrorist attacks should be improved by creating a public-health reserve system and by developing surge capacity to deal effectively with such terrorist attacks as well as with natural catastrophes. Additionally, new strategies must be developed and implemented for assuring the security, usability, and accurate documentation of existing stocks of supplies at research facilities, hospitals, veterinarian facilities, and other host sites. The potential for a major infectious threat to kill and disable thousands of citizens requires a level of preparedness that we currently lack—a surge capacity to mobilize the public-health response and provide emergency care in a health system that has been somewhat downsized in an effort to cut costs. There are immediate needs and opportunities for training first responders, medical, nursing, and health professionals, and communities as a whole in how to respond to biological threats. Also needed is a well-trained, professional public-health reserve, including laboratories and health personnel, that can be mobilized. Standardized protocols for such purposes will be critically important.

## Toxic Chemicals and Explosive Materials

The toxic, explosive, and flammable properties of some chemicals make them potential weapons in the hands of terrorists. Many such chemicals (e.g., chlorine, ammonium nitrate, and petroleum products) are produced, transported, and used in large quantities. Chemical warfare agents (such as nerve and blister agents) developed to have extremely high toxicities have been incorporated into a variety of military weapons. These chemical weapons could become available to terrorists through purchase or theft. Some of the chemical agents themselves are not difficult for individuals or organized groups to make.

In principle a number of technologies can be brought to bear for the rapid detection and characterization of a chemical attack, or for detecting explo-

sives before they are used. Large investments have been made in research on sensor technologies, but to date the number of effective fielded systems developed remains comparatively small. If sensor research is to move forward efficiently, mechanisms to focus and exploit the highly fragmented array of existing research and development programs will be needed. **A new program should be created to focus and coordinate research and development related to sensors and sensor networks, with an emphasis on the development of fielded systems.** This program should build on relevant sensor research under way at agencies throughout the federal government.

Research programs on sensor technologies are needed to continue the search for promising new principles on which better sensors might be based. For example, mass spectroscopy offers the possibility of very rapid and specific identification of volatile agents. Also, basic research on how animals accomplish both detection and identification of trace chemicals could yield new concepts that allow us to manufacture better sensor systems and reduce our dependence on trained dogs, which currently are the best broad-spectrum high-sensitivity sensory systems.

Toxic chemicals (or infectious agents) could be used by terrorists to contaminate food production facilities or water supplies. Although a good deal of attention has been paid to ensuring safety and purity throughout the various stages of food production, processing, and distribution, protecting the food supply from intentional contamination has not been a major focus of the U.S. food industry. **The FDA should develop criteria for quantifying hazards in order to define the level of risk for various kinds of food-processing facilities.** The results could be used to determine the minimal level of protection required for making each type of facility secure. **The FDA should also act promptly to extend the current quality control approach (Hazard Analysis and Critical Control Point methodology) so that it might be used to deal effectively with deliberate contamination of the food supply.**

One of the best ways to secure the safety of the water supply is to ensure an adequate residual concentration of disinfectant (usually chlorine) downstream of water treatment plants, although more information is needed to be able to do this well. **The EPA should direct additional research on determining the persistence of pathogens, chemical contaminants, and other toxic materials in public water supplies in the presence of residual chlorine.**

Once a release of toxic chemicals occurs, proper protection of people and buildings can do a great deal to reduce injury and facilitate cleanup and recovery. **Universities, companies, and federal agencies need to work together to advance filtering and decontamination techniques by both improving existing technologies and developing new methods for removing chemical contaminants from air and water.** Research is especially needed on filter systems capable of treating large volumes, novel media that can help prevent toxic materials from entering facilities through ventilation equipment and ducts, and methods to contain and neutralize clouds of airborne toxic materials. In addition, exploratory programs should be initiated in new approaches to decontamination, including hardened structures, protective systems for microelectronics and other expensive equipment, and environmentally acceptable ways of disposing of contaminated material that cannot be cleaned.

New technologies that offer significant advances should be constantly evaluated. But the process of evaluating different sensor systems, for example, is difficult because their effectiveness depends on the operational environment and on who will be using them. **Because a bewildering array of counterterrorism technologies (including various kinds of sensor systems, filters, and decontamination methods) are being developed, programs to determine standards and to support technology testing and performance verification are needed. These programs should be designed both to help guide federal research investments and to advise state and local authorities on the evolving state of the art.**

## Information Technology

The three counterterrorism-related areas of highest priority in information technology (IT) are information and network security, information technologies for emergency response, and information fusion and management. In particular, immediate actions should be taken on the critical need to improve the telecommunications and computing infrastructure of first responders and to promote the use of best practices in information and network security, especially by emergency response agencies and telecommunications providers.

All of the research areas outlined here and in Chapter 5 are critically relevant to the nation's counterterrorism effort, but it should be noted that progress in them could also be applied to a wide range of other important national endeavors, such as responses to natural disasters.

Attacks on information technology can amplify the impact of physical attacks and diminish the effectiveness of emergency responses. Reducing such vulnerabilities will require major advances in computer security, with the objective of consequently improving information and network security. Furthermore, reliance on the Internet as the primary networking entity means that severe damage through cyberattacks is more likely. **The administration and Congress should decide which agency is to be responsible for promoting information security in the federal government through the adoption and use of what is currently known about enhancing security practices.** To the extent that the federal government is successful in improving its procedures, it should make these best practices available to other elements of government and to the private sector.

Command, control, communications, and information (C3I) systems for emergency responders are critical for coordinating their efforts and increasing the promptness and effectiveness of response. Unfortunately, such systems are extremely vulnerable to attack; currently many of them do not even use state-of-the-art mechanisms for security and reliability. **Since emergency-response organizations often do not have the expertise to review and revamp the telecommunications and computing technologies used for emergency response, it is necessary to provide them with authoritative knowledge and support. In addition, designated emergency-response agencies should use existing technology to achieve short-term improvements in the telecommunications and computing infrastructure for first responders.**

All phases of counterterrorism efforts require that large amounts of information from many sources be acquired, integrated, and interpreted. Given the range of data sources and data types, the volume of information each source provides, and the difficulty of analyzing partial information from single sources, the timely and insightful use of these inputs is very difficult. Thus, information fusion and management techniques promise to play a central role in the future prevention, detection, and remediation of terrorist acts.

Unlike some other sectors of national importance, information technology is a sector in which the federal government has little leverage. Thus, constructively engaging the private sector by emphasizing market solutions seems a desirable and practical way for the government to stimulate advances that can strengthen the nation's information technology infrastructure. The challenge for federal policy makers is to change the market dynamics by encouraging the private sector to pay more attention to security-related issues and by facilitating the adoption of effective security (e.g., through federally supported or incentivized research that makes better technologies available and reduces the costs of implementing security-related functionality).

Within the federal government, numerous federal agencies, including DOD (and especially DARPA), NSF, NIST, and the DOE national laboratories, all play important roles in funding and performing telecommunications and computing research, and many other agencies are major users of IT. **A strategic long-term research and development agenda should be established to address three primary counterterrorism-related areas in IT: information and network security, the IT needs of emergency responders, and information fusion.** The R&D in information and network security would include but not be limited to approaches and architectures for prevention, identification, and containment of cyberintrusions and recovery from them. The R&D to address IT needs of emergency responders would include but not be limited to ensuring interoperability, maintaining and expanding communications capacity in the wake of a terrorist incident, communicating with the public during an emergency, and providing support for decision makers. The R&D in information fusion for the intelligence, law enforcement, and emergency response communities should include but not be limited to data mining, data integration, language technologies, and processing of image and audio data.

The federal government's efforts should focus on multidisciplinary problem-oriented research that is applicable to both civilian and military users, yet is driven by a deep understanding and assessment of vulnerabilities to terrorism. To achieve long-term advances, the research must extend beyond improving existing systems and investigate new approaches to secure and reliable operation that do not directly evolve from the information technology of today.

## Energy Systems

Energy systems include the country's electrical supply system and its oil and gas facilities. The electrical system warrants special attention in that a prolonged loss of service to a region would probably cause extensive hardships, economic loss, and many deaths. Outage of an entire regional transmission grid might occur if the damage or destruction of important components of that grid were followed by a cascading failure of interconnected components. To reduce near-term vulnerability to such a loss, **those parties responsible for critical components of the electric-power grid should be urged to install physical barriers, where they do not already exist, to protect these components. In the longer term, the Department of Energy, through its national laboratories and supported by other government agencies and significant industry participation, should take the lead in developing, testing, and implementing an intelligent, adaptive electric-power grid.** Such an intelligent grid would provide the system with the ability to fail gracefully, minimizing damage to components and enabling more rapid recovery of power. A key element would be adaptive islanding, a concept employing fast-acting sensors and controls to isolate parts of the power system. Operations models and intelligence would be needed to differentiate between failure of a single component and the kind of concurrent or closely coupled serial failures, at several key nodes, that could indicate the onset of a concerted attack.

Another vulnerability of the power grid is its extra-high-voltage transformers, for which the country stocks limited numbers of replacements. Replacement of a seriously damaged or destroyed unit could take months or even years. To counter this vulnerability, **research and development should be undertaken by DOE and the electric power industry to determine if a modular, universal, extra-high-voltage transformer might be developed to provide temporary replacement when key components are damaged.** These replacement transformers would be relatively small, easily transported, and capable of being used individually or in sets to replicate the unit being replaced.

Yet another challenge is the vulnerability of the power grid's control systems to cyberattack. In particular, the supervisory control and data acquisition (SCADA) systems pose a special problem. As a result, **the manner in which data are transmitted between control points or SCADA systems used in the**

**grid should be reviewed. Encryption techniques, improved firewalls, and cyberintrusion-detection technologies should be used to improve security and reduce the potential for hacking and disruption.** Because oil and gas systems (and non-energy systems) are similarly vulnerable, this recommendation applies to those facilities as well.

The country's electric-power transmission grids and oil and gas pipelines extend over thousands of miles and in many cases are quite remote, thus complicating observation and supervision. Therefore **existing surveillance technologies developed for defense and intelligence applications should be investigated for their usefulness in defending against terrorist attacks, as well as against simple right-of-way encroachments, on widely distributed oil, gas, and electrical transmission assets.**

The dependence of major infrastructural systems on the continued supply of electrical energy, and of oil and gas, is well recognized. Telecommunications, information technology, and the Internet, as well as food and water supplies, homes, and worksites, are dependent on electricity; numerous commercial and transportation facilities are also dependent on natural gas and refined oil products. These and many other interdependencies need to be better understood in order to determine which nodes of the various energy systems should be given the highest priority for increased security against terrorism. Simulation models of interdependent infrastructures may help provide such understanding and also prove vital to post-event recovery. Therefore new and improved simulation-design tools should be developed to model and analyze prevention, response, and recovery for energy systems under a variety of terrorist-threat scenarios. These efforts would include simulations of the interdependencies between the energy sector and key infrastructures such as the communication, transportation, and water-supply systems.

## Transportation Systems

Transportation security is best achieved through well-conceived security systems that are integrated with transportation operations. A layered security system, in which multiple security features are connected and provide backup for one another, has particular advantages. Defeating a single layer cannot

breach such systems, and the difficulty of calculating the overall odds of success may thus deter as well as impede terrorist attacks. Moreover, layered security features that are well integrated with operations and confer multiple benefits, such as enhanced safety and operating efficiency, are likely to be maintained and improved over time.

Many actions are now being taken by the federal government to strengthen air transportation security—from the deployment of explosives-detection systems for checked baggage to the strengthening of cockpit doors to the use of air marshals. Some of these measures are providing much-needed security layers, although not yet as part of a preconceived system designed to address multiple threats and ensure continued improvement over time. Likewise, new security approaches are being considered for marine shipping containers, particularly the possibility of moving inspections out from the U.S. ports of entry and farther down the logistics chain. For these two critical parts of the transportation sector well-conceived security systems must be put in place soon, and research and development are essential for further improving these systems.

Many of the areas recommended for R&D in this report—such as improved sensors, the ability to mine data more effectively, and especially a capability for unconventional, broad-based thinking on terrorist threats and responses—will also be of great value in boosting security for transportation and distribution. However, **the most critical need in the transportation sector is a systematic approach to security. The new Transportation Security Administration (TSA) is positioned to help meet this need by serving as a focal point of responsibility for devising effective and coherent security systems for each transportation mode and by supporting and marshaling relevant R&D.** TSA presents an unprecedented opportunity to build security into the nation's transportation sector in a more methodical way; indeed, Congress has chartered TSA to take on such a strategic role.

Compelled to act quickly in enhancing civil aviation security, TSA is now beginning to examine the security needs of all transport modes and to define its own role in meeting them. **To help meet its obligation to strengthen security in all transportation modes, TSA should create a multimodal, strategic research and planning office.** Further, to increase the utility of sensing, decontamination, screening, and other security-related technologies being developed, TSA must have its own research capacity as well as the ability to work with and

draw on expertise from both inside and outside the transportation community. By working constructively with the Department of Transporta-tion's modal agencies (such as the Federal Aviation Administration and the Federal Highway Administration), other federal entities, state and local government, and the private sector, this recommended office can serve as a focal point for research, planning, and collaboration. It will be positioned to identify and evaluate promising security-system concepts as well as to promote the development of knowledge, technologies, and processes for implementing them.

Within DOT, the individual modal agencies and the Volpe National Transportation Systems Center offer important resources for systems-level research and for technology development. TSA can help guide their investments to better leverage the transportation sector's own R&D investments and ensure their strong security relevance. By making the needs and parameters of transportation-security systems more widely known, especially to the much larger R&D community and sponsoring agencies in government, TSA can help to identify and shape the efforts that are most promising and relevant.

Because the identification of appropriate security systems is essential to guiding related technology development and deployment, **TSA should take the lead in devising and evaluating a set of promising security system concepts for each transportation mode.** The diverse operators, users, and overseers in the transportation sector—public and private alike—must ultimately deploy and operate the security systems; however, their disparate venues and interests can hinder cooperation in the development of alternative system concepts. TSA, through the recommended strategic research and planning office, is particularly well placed to encourage and orchestrate such cooperation.

By working with transportation system owners, operators, and users in exploring alternative security concepts, TSA will be better able to identify opportunities for conjoining security with other objectives, such as improving shipment and luggage tracking. Such multiuse, multibenefit systems have a greater chance of being adopted, maintained, and improved.

The agency will also become more sensitive to implementation issues—from technological and economic factors to political and societal challenges—as evaluations help gauge the need for changes in laws, regulations, financial incentives, and divisions of responsibility among public and private entities. Some of these indicated changes may be practical to achieve; others may not.

The prospects of deploying many new technologies and processes in support of security systems, from biometric ID cards to cargo- and passenger-screening devices, will also raise many difficult social issues—concerns over legality, personal privacy, and civil rights, for example. Concerns that may constrain or even preclude implementation must be appreciated early on, before significant resources are devoted to furthering impractical or undesirable concepts.

As TSA seeks to develop and deploy security system concepts, consideration of human factors will be critical. Human factors expertise is necessary for crafting layered security systems that, as a whole, increase the perceived risk of getting caught and maximize the ability of security personnel to recognize unusual and suspicious patterns of activity and behavior. **Recognition of human factors is important for ensuring that the role of people in providing security is not determined by default on the basis of what technology promises, but rather as a result of systematic evaluations of human strengths and weaknesses that technology can both complement and supplement. TSA can take the lead in making sure that human factors are fully considered in all security initiatives and at the earliest possible stages.**

## Cities and Fixed Infrastructure

American cities present a target-rich environment for the terrorist. The urban setting provides access to a set of highly integrated infrastructure systems—such as water, electrical, and gas supplies; communications; and mass transit—as well as to numerous major buildings and places of public assembly.

Major buildings have been recognized as especially attractive targets, and, based on the events of September 11, they have also become the subject of serious structural reexamination—in particular, to determine what weaknesses must be corrected to prevent catastrophic collapse following an attack, as happened with the twin towers of the World Trade Center. Study of the information coming from the failure of those buildings indicates that **research and development leading to improved blast- and fire-resistant designs should be undertaken by NIST, the national laboratories, Underwriters Laboratories, the National Fire Protection Association, and appropriate code-writing organizations. In the near term, while results of this research and development are being realized, provisional guidelines may be issued that are based on the more**

**advanced fire-rating practices now employed in Europe, Australia, and New Zealand.** The results of this work should be disseminated so that new knowledge is incorporated into the codes and standards for the design and construction of new buildings, and for remodeling the existing stock as well. Specific testing programs are recommended in Chapter 8, with particular attention given to methods and materials for fire protection and to connections and curtain walls.

Major buildings are also vulnerable to infectious or toxic materials being circulated by heating, ventilation, and air-conditioning (HVAC) systems after their release into the air. To counter this threat, it is necessary that NIST, perhaps together with other agencies and the national laboratories, undertake a research and development program for sensors that can be installed in the air-handling ducts. These sensors could determine whether air is safe or not, and allied controls could adjust the functioning of HVAC systems accordingly.

The heart of a city's response to a terrorist attack is an emergency operations center (EOC) and the first responders—those who are typically dispatched to the scene of a problem before the EOC can determine its nature or cause. **An urgent near-term task is to develop credible terrorist-threat scenarios that EOC teams can prepare to meet. Further, a technical assessment of the adequacy of an EOC's physical facilities to address and survive these threat scenarios should be performed.**

The ability of first responders to quickly determine if the dust and smoke at a site contain toxins will likely mean the difference between life and death. **It is important that research and development be undertaken with the aim of producing new, small, reliable, and quick-reading sensors of toxic materials for use by first responders.** These devices might be based on the same core element as the sensors recommended for HVAC systems.

EOC crisis management teams around the country have had experience in dealing with natural disasters and perhaps some human-made threats (such as riots) to cities, but very few have had any experience in dealing with a terrorist attack. This lack of experience, and the potential problems it implies for attack recognition, response, interagency operations, and public information management and media relations, are a serious vulnerability. **OHS and FEMA, in conjunction with state and local officials, should collaborate to develop and deploy threat-based simulation models and training modules for**

**EOC training, for identification of weaknesses in systems and staff, and for testing and qualifying EOC teams throughout the country.**

## The Response of People to Terrorism

Most thinking and planning related to preparedness, warning, and response rests on the assumption of an undifferentiated "community" or "public." Research on disasters, however, reveals that individuals and groups differ in both readiness and response according to previous disaster experience, ethnic and minority status, knowledge of the language, level of education, level of economic resources, and gender. In addition, individual households vary in their responses to crises, depending on factors such as perceived risk, credibility of warning system, and concerns about family and property. The behavioral and social sciences can thus make important contributions to understanding group responses to crises. **A program of research should be established to understand how differences based on cultural background, experience with previous disasters, and other factors should be taken into account when systems are designed for preparedness, warning, and response to terrorist attacks and other disaster situations.** A basic research program in the National Science Foundation could build the groundwork for this counterterrorism research.

While research will lay the groundwork for long-term improvements in the quality of preparedness, warning, and response communications, in the near term the government must be preparing now to communicate as best it can in the aftermath of a crisis. **Appropriate and trusted spokespeople should be identified and trained now so that, if a terrorist attack occurs, the government will be prepared to respond not only by supplying emergency services but also by providing important, accurate, and trustworthy information clearly, quickly, and authoritatively.**

To strengthen the government's ability to provide emergency services, in-depth research should be conducted to characterize the structure of agencies responsible for dealing with attacks and other disasters. These studies would focus on discovering optimal patterns of information dissemination and communication among the agencies, the most effective strategies for coordination

under extreme conditions, ways of responding to the need for spontaneous and informal rescues, and approaches to dealing with citizen noncooperation. Research should also focus on the origins and consequences of organizational failure, miscommunication, lack of coordination, and jurisdictional conflict. Comparative work on cases of successful coordination should also be prominent on the research agenda. **NSF, FEMA, and other agencies should support research—basic, comparative, and applied—on the structure and functioning of agencies responsible for dealing with attacks and other disasters.**

The interface between technology and human behavior is an important subject for investigation. The research agenda should be broad-based, including topics such as decision making that affects the use of detection and prevention technologies; the ways in which deployment of technologies can complement or conflict with the values of privacy and civil liberty; and factors that influence the trustworthiness of individuals in a position to compromise or thwart security. **All the agencies creating technological systems for the support of first responders and other decision makers should base their system designs and user interfaces on the most up-to-date research on human behavior, especially with respect to issues critical to the effectiveness of counterterrorism technologies and systems.**

## Complex and Interdependent Systems

A major theme of this report is the need for an overall systems approach to counterterrorism. But many of the U.S. government's departments and agencies do not have the capabilities needed to assess terrorist threats, infrastructure vulnerabilities, and mitigation strategies from a systems perspective. For example, **in order to perform the analyses needed to identify vulnerabilities in complex systems and weaknesses due to interconnections between systems, various threat and infrastructure models must be extended or developed, and used in combination with intelligence data.** A systems approach is especially necessary for understanding the potential impacts of multiple attacks occurring simultaneously, such as a chemical attack combined with a cyberattack on first responder communications designed to increase confusion and interfere with the response.

The required range of expertise is very broad. Information about threats must come from communities knowledgeable about chemical, biological, and nuclear weapons and information warfare, while vulnerability analysis will depend on information about critical infrastructures such as the electric power grid, telecommunications, gas and oil, banking and finance, transportation, water supply, public health services, emergency services, and other major systems. In all these areas **threat assessments and red-team activities will be essential.**

Currently, there is a large volume of information collected and analyzed by the U.S. intelligence community and in industry that is relevant to assessing terrorist threats and system vulnerabilities. However, to maximize the usefulness of this data and increase the ability to cross-reference and analyze it efficiently, **counterterrorism-related databases will have to be identified and metadata standards for integrating diverse sets of data established.**

Important information about vulnerabilities can also be gained by modeling of critical infrastructures. Computational or physical-analog models of infrastructure for use in simulating various counterterrorism activities can help with identifying patterns of anomalous behavior, finding weak points in the infrastructure, training personnel, and learning how to maintain continuity of operations following terrorist attacks. **Existing modeling and analysis capabilities, as well as new methods, could allow the use of integrated models to determine linkages and interdependencies between major infrastructure systems.** These results, in turn, could be used to develop sensor-deployment strategies and infrastructure-defense approaches in areas of major vulnerability.

The basic tools of systems analysis and modeling are available today and are widely used in military and industrial applications. But these tools have severe limitations when applied to interdependent complex systems, and research is required to extend them. Thus a long-term research agenda in systems engineering should be established by the federal government. Relevant research projects will involve many domains of expertise; a single disciplinary perspective should not dominate the agenda. Relevant initiatives would focus on the following:

- System-of-systems perspectives for homeland security;

- Agent-based and system-dynamics modeling;
- Analysis of risk assessment and management from multiple perspectives, including the risk of potentially extreme and catastrophic events;
- Modeling of interdependencies among critical infrastructures; and
- Development of simulators and learning environments.

## The Significance of Crosscutting Challenges and Technologies

The survey of key vulnerabilities and potential solutions outlined above and discussed in greater detail in Chapters 2 to 10 reveals a striking set of crosscutting issues. Apparent in more than one of the areas examined, these issues make it clear that countering terrorism will require insights and approaches that cut across traditional boundaries of scientific and engineering disciplines. Seven crosscutting challenges were identified by the committee: systems analyses, modeling, and simulation; integrated data management; sensors and sensor networks; autonomous mobile robotic technologies; supervisory control and data acquisition (SCADA) systems; control of access to physical and information systems using technologies such as biometrics; and human and organizational factors.

Systems analysis and modeling tools are required for threat assessment; identification of infrastructure vulnerabilities and interdependencies; and planning and decision making (particularly for threat detection, identification, and response coordination). Modeling and simulation also have great value for training first responders and supporting research on preparing for, and responding to, biological, chemical, and other terrorist attacks.

As the intelligence problems prior to September 11 demonstrate, ways to integrate and analyze data are required to support intelligence activities as well as development and use of comprehensive, systems-based defenses for the nation's cities and infrastructures. New data management standards and techniques will also be required.

The development and use of sensors and sensor networks will be critical for the detection of conventional, biological, chemical, nuclear, and information-warfare weapons and means for their delivery. To be effective and acceptable for operational use, these systems must operate at appropriate levels of

sensitivity and specificity to balance the danger of false negatives and the disruption caused by false positives.

Continued development and use of robotic platforms will enable the deployment of mobile sensor networks for threat detection and intelligence collection. Robotic technologies can also assist humans in such activities as ordnance disposal, decontamination, debris removal, and firefighting.

Supervisory control and data acquisition (SCADA) systems are widely used for managing and monitoring most components of the nation's basic infrastructures. Effective security for these systems is not currently well defined, much less implemented.

In many areas, effective security will depend on controlling people's access to physical and information systems while not adversely affecting the performance of these systems. Biometrics is one example of how technology might be used to achieve more effective and less disruptive security systems.

All of the technologies discussed in this report are critically important, but none of them is the sole solution to any problem. Because technologies are implemented and operated by human agents and social organizations, their design and deployment must take human, social, and organizational factors into account.

## Realizing the Potential of Science and Technology to Counter Catastrophic Terrorism

The recommendations offered in this report should not be judged or acted upon individually. It is important instead that the federal government define a coherent overall strategy for protecting the nation, harness the strengths of the U.S. science and engineering communities, and direct them most appropriately toward critical goals, both short term and long. Chapter 12 identifies the steps needed in the federal government (both in the White House and in the agencies that contribute to homeland security) to ensure that today's technological counters to terrorism are fielded and tomorrow's solutions are found. Chapter 13 describes the important roles of the federal government's partners in homeland security efforts: state and local governments, industry, universities, not-for-profit laboratories and organizations, and other institutions.

## Capabilities Needed to Develop a Counterterrorism Strategy and Effectively Deploy Technology

Research performed but not exploited, and technologies invented but not manufactured and deployed, do not help the nation protect itself from the threat of catastrophic terrorism. In this report, the committee urgently recommends a number of steps to ensure that technical opportunities are properly realized. In particular, in recognition of the importance and difficulty of determining goals and priorities, the committee discusses how the federal government might gain access to crucial analytic capabilities to inform decision making—allowing improved assessment of risk and of the effectiveness of measures to counter risk.

Most important is that there be a federal office or agency with central responsibility for homeland security strategy and coordination and that this organization have the structure and framework necessary to bring responsibility, accountability, and resources together to effectively utilize the nation's science and engineering capabilities. The committee believes that the technical capabilities to provide the analysis necessary to support this organization do not currently exist in the government in a unified and comprehensive form. Thus **the committee recommends the creation of a Homeland Security Institute to serve the organization setting priorities for homeland security.**

This institute would provide systems analysis, risk analysis, and simulation and modeling to determine vulnerabilities and the effectiveness of the systems deployed to reduce them; perform sophisticated economic and policy analysis; manage red-teaming activities; facilitate the development of common standards and protocols; provide assistance to agencies in establishing testbeds; design and use metrics to evaluate the effectiveness of homeland security programs; and design and support the conduct of exercises and simulations. The committee believes that to function most efficiently, this institute should be located in a dedicated, not-for-profit, contractor-operated organization.

In the current structure, the primary customer for this Homeland Security Institute would be the Office of Homeland Security, which is currently responsible for producing a national homeland security strategy. Whether this office will also be responsible for monitoring progress on this strategy and revising it in the future is not clear. On June 6, 2002, the President proposed

a reorganization in which many of the agencies and programs operating on the front line of counterterrorism would be brought together to form a new Department of Homeland Security. However, even within this department, the programs with the expertise and experience in science and engineering research would not necessarily be closely connected to the units with the responsibility for technology deployment. Perhaps more important, the federal agencies with the best access to the nation's sources of scientific, engineering, and medical research capability lie outside the proposed department, and close connections with these groups will be needed to allow the department to produce the best-quality effort on counterterrorism.

Thus, however the leadership of the federal effort in homeland security is organized, the government will need mechanisms to engage the technical capabilities of the government and the nation's scientific, engineering, and medical communities in pursuit of homeland security goals. Today the focus is on determining these goals, and the link between the Office of Homeland Security and the Office of Science and Technology Policy is a key element in setting the science and technology component of the national counterterrorism strategy. This link will continue to be essential, but if a new department is formed it will not be enough. A new department will need an Undersecretary for Technology to provide a focal point for guiding key research and technology development programs within the department and connecting with relevant technology agencies outside it. In addition, the Office of Homeland Security will need to work closely with the Office of Science and Technology Policy, perhaps through the National Science and Technology Council, on coordinating multiagency projects and their linkages to related programs devoted primarily to other high-priority national objectives.

## Essential Partners in a National Strategy: States and Cities, Industry, and Universities

The federal government must take the lead in the national counterterrorism effort, but effective use of existing technologies, research and development activities, and deployment of new approaches to mitigating the nation's vul-

nerabilities will depend critically on close cooperation with other entities: non-federal governments, industry, universities, not-for-profit laboratories and organizations, and other institutions.

Primary responsibility for response to and recovery from terrorist attacks will fall to cities, counties, and states. The first responders (police, firefighters, and others) and local governments possess practical knowledge about their technological needs and relevant design limitations that should be taken into account in federal efforts to provide new equipment (such as protective gear and sensor systems) and help set standards for performance and interoperability. Federal agencies will have to develop collaborative relationships with local government and national organizations of emergency services providers to facilitate technological improvements and encourage cooperative behavior.

Private companies own many of the critical infrastructures that are targets for terrorism. Inducing industry to play its critical role in homeland security activities—to invest in systems for reducing their vulnerabilities and to develop and manufacture counterterrorism technologies that may not have robust commercial markets—may require new regulatory requirements, financial incentives, and/or voluntary consensus agreements. A public-private dialogue is required to define the best approach for particular industrial sectors and types of vulnerabilities.

Sustaining a long-term national effort against terrorism will require minimizing the costs of security efforts and avoiding as much as possible placing extra burdens on accustomed conveniences or constraints on civil liberties. Most of the recommendations in this report, if acted on, will not only make the nation safer from terrorist attacks but can also make it safer from natural disasters, infectious diseases, hackers disrupting the Internet, failures in electric power distribution and other complex public services, and human error causing failures in such systems. This promise will help sustain the public's commitment to addressing the terrorism threat, and suggests that it is not inappropriate that many of the research and development programs to counter terrorism should be pursued in close coordination with similar efforts to improve the quality of life in civil society.

Indeed, America's historical strength in science and engineering is perhaps its most critical asset in countering terrorism without degrading our quality of

life. It is essential that we balance the short-term investments in technology intended to solve the problems that are defined today with a longer-term program in fundamental science designed to lay foundations for countering future threats that we cannot currently define. These long-term programs must take full advantage of the nation's immense capacity for performing creative basic research, at universities, government laboratories, industrial research facilities, and non-governmental organizations. A dialogue should take place between the federal government and the research universities on how to balance the protection of information vital to national security with the requirement for a free and open environment in which research is most efficiently and creatively accomplished. This dialogue should take place before major policy changes affecting universities are enacted.

The nation's ability to perform the needed short- and long-term research and development rests fundamentally on a strong scientific and engineering workforce. Here there is cause for concern, as the number of American students interested in science and engineering careers is declining, as is the support for physical science and engineering research. A dialogue should take place between the federal government and the research universities on how best to reverse this human resource trend. If the number of qualified foreign students declines, the need to reverse this trend will become even more urgent. The committee is not suggesting that the United States alone should provide all of the needed counterterrorism science and technology. While this report focuses almost exclusively on potential U.S. actions, it is critical to emphasize that many other nations are vulnerable to the same terrorist threats, and they have valuable technical skills to contribute to the mitigation of vulnerabilities. The world will become safer, faster, if the scientific and engineering contributions to counterterrorism are based on cooperative international efforts.

# Transportation Panel Biographical Information

**Mortimer L. Downey,** *Chair*, is former U.S. Deputy Secretary of Transportation and now principal consultant with PBConsult, the management consulting subsidiary of Parsons Brinckerhoff. As Deputy Secretary from 1993 to 2001, Mr. Downey was the U.S. Department of Transportation's Chief Operating Officer. He also served on the President's Management Council, as Chairman of the National Science and Technology Council Committee on Transportation Research and Development, and as a member of the Board of Directors of Amtrak. Previously, Mr. Downey was Executive Director and Chief Financial Officer of New York's Metropolitan Transportation Authority, the nation's largest independent public authority. He is well known for developing innovative solutions to complex public policy issues, and has championed a systemwide approach to transportation decision making. Mr. Downey serves as chairman of the Board of Directors of the National Academy of Public Administration and as a board member of the Eno Transportation Foundation. He has received the Frank Turner Lifetime Achievement Award from the Transportation Research Board (TRB), the Lifetime Achievement Award from the American Public Transportation Association, and the Leadership Award from ITS America.

**H. Norman Abramson** is Executive Vice President Emeritus, Southwest Research Institute. He is internationally known in the field of theoretical and applied mechanics. His specific area of expertise is the dynamics of contained liquids in astronautical, nuclear, and marine systems. He began his career as Associate Professor of Aeronautical Engineering at Texas A&M University and has since served as Vice President and Governor of the American Society of Mechanical Engineers and Director of the American Institute of Aeronautics and Astronautics (AIAA). He is an AIAA Fellow and Fellow and Honorary Member of the American Society of Mechanical Engineers. As

a member of the National Academy of Engineering (NAE), he served on its council from 1984 to 1990. He has also served on many other NAE and National Research Council (NRC) committees, including the Commission on Engineering and Technical Systems (CETS) Committee on R&D Strategies to Improve Surface Transportation Security, on which he served as chairman; TRB's Research and Technology Coordinating Committee; and TRB's Committee on the Federal Transportation R&D Strategic Planning Process. He also served as a member of the U.S. Air Force Scientific Advisory Board from 1986 to 1990.

**Lisa M. Bendixen** is principal in the Global Environment and Risk Division of ICF Consulting, LLC, specializing in safety and risk. Since joining the division previously owned by Arthur D. Little, Inc., she has been involved in risk management and risk assessment studies conducted within numerous industries, covering both fixed facilities and transportation systems. She was project manager for and primary author of *Guidelines for Chemical Transportation Risk Analysis*, published by the American Institute of Chemical Engineers' Center for Process Safety. She served on TRB's Committee on Fiber Drum Packaging for Transporting Hazardous Materials. She is currently a member of the Committee for the Review and Evaluation of the Army Non-Stockpile Chemical Materiel Disposal Program.

**Anthony J. Broderick** is an independent aviation safety consultant who works with international airlines, aerospace and aircraft manufacturing firms, and national governments. Before retiring from his post as Associate Administrator for Regulation and Certification at the Federal Aviation Administration (FAA), he served for 11 years as the federal government's senior career aviation safety official. He led FAA's development of the International Aviation Safety Assessment program, and was instrumental in leading international efforts to establish certification and operational standards for safety. Prior to becoming Associate Administrator, he spent 14 years in FAA and the U.S. Department of Transportation (DOT) and 7 years in private industry. He has an extensive background in civil aviation safety, security, and environmental issues. He is a member of NRC's Aeronautics and Space Engineering Board.

**Noel K. Cunningham** is Director of Operations for the Port of Los Angeles. In this position, which he has held since 1994, he manages the Port Police, Port Pilot, and Emergency Management Divisions. He serves as Chief of Police for the Port of Los Angeles, the only U.S. police force dedicated to port activities, which enforces all federal, state, and local laws applicable to cargo protection, pollution investigations, vessel traffic control, and drug interdiction. He is immediate past President of the International Association of Airport and Seaport Police. Before joining the Port of Los Angeles in 1991, he served as an area captain with the Los Angeles Police Department for 25 years.

**John J. Fearnsides** is Professor of Public Policy at George Mason University and a Senior Strategic Consultant with Lockheed Martin Corporation. Until 1999, he was Senior Vice President and General Manager of The MITRE Corporation and Director of its Center for Advanced Aviation System Development, which is sponsored by FAA. He worked at DOT from 1972 to 1980, serving as Deputy Under Secretary and Chief Scientist, Executive Assistant to the Secretary, and Acting Assistant Secretary for Policy and International Affairs. He was a National Science Foundation Fellow and is a Fellow of the Institute of Electrical and Electronics Engineers and the National Academy of Public Administration. He has served as a member of numerous NRC and TRB committees, including most recently the Committee for a Study of the Public Sector Requirements for a Small Aircraft Transportation System.

**Stephen E. Flynn** is Commander, U.S. Coast Guard, and Senior Fellow, National Security Studies Program, Council on Foreign Relations. As a Commander in the Coast Guard, he is a member of the Permanent Commissioned Teaching Staff at the U.S. Coast Guard Academy. Currently at the Council on Foreign Relations, he is directing a multiyear project on Protecting the Homeland: Rethinking the Role of Border Controls. He has served in the White House Military Office and as a Director for Global Issues on the National Security Council staff. He is the author of several publications on border control, homeland security, the illicit drug trade, and trans-

portation security, including "America the Vulnerable," published in *Foreign Affairs* in 2002, and "The Unguarded America," which appears in a collection of essays on the September 11 attacks published by Public Affairs Books. He has been a Guest Scholar in the Foreign Policy Studies Program at the Brookings Institution and Annenberg Scholar-in-Residence at the University of Pennsylvania.

**Francis B. Francois** retired in 1999 as Executive Director of the American Association of State Highway and Transportation Officials (AASHTO). Previously, he was a member of the County Council of Prince George's County, Maryland, an elected position in which he was involved in transportation, public works, environmental, and community development issues. In his capacity as AASHTO Executive Director, he was an active participant in and supporter of TRB activities, including the TRB Executive Committee and the Strategic Highway Research Program. He was recently a member of the Committee for a Study for a Future Strategic Highway Research Program and is currently a member of TRB's Task Force on Critical Transportation Infrastructure Protection. He is a member of the National Academy of Engineering.

**Ernest R. Frazier, Sr.,** is Vice President of the System Security and Safety Department of the National Railroad Passenger Corporation. In this position, he serves as Chief of Police and is responsible for the oversight, development, and implementation of the corporation's systemwide security and safety initiatives. He has been a law enforcement officer for 25 years and with Amtrak since 1981, appointed as Chief of Police in 1994. During his tenure, the Amtrak Police Department became the first law enforcement agency with additional jurisdictional responsibility to achieve national accreditation as a police force. He is a member of the International Association of Chiefs of Police and has served on its Terrorism Committee. He is past President and a current member of the International Association of Railway Police and past Chairman of the Railroad Police Section of the International Association of Chiefs of Police and the United States Department of Justice Transportation Security Subcommittee.

**Robert E. Gallamore** is Director of the Transportation Center and Professor of Managerial Economics and Decision Sciences in the Kellogg Graduate School of Management, Northwestern University. Prior to joining the university in August 2001, he was an executive on loan from Union Pacific Railroad to the Transportation Technology Center in Pueblo, Colorado. At Union Pacific, he was Assistant Vice President of Communications Technologies and General Manager of the North American Joint Positive Train Control Program. He has also served in several positions with the federal government, including Deputy Federal Railroad Administrator and Associate Administra-tor for Planning of the Urban Mass Transportation Administration.

**Henry L. Hungerbeeler** is Director of the Missouri Department of Transportation, overseeing the work of 6,000 employees and a system that includes 32,000 miles of highway, as well as state-aided airports, transit systems, railroads, and ports. Before joining the department, he spent his career in the U.S. Air Force, serving as chief of staff for the military task force combating international drug cartels. He also served as base commander for Charleston Air Force Base and Andrews Air Force Base. He trained and led the security force that protected Air Force One. He is currently Chairman of AASHTO's Task Force on Transportation Security.

**Brian M. Jenkins** is Senior Advisor to the President of RAND Corporation. He also is a Research Associate in the Mineta Transportation Institute at San Jose State University, and until 1998 was Deputy Chairman of Kroll Associates. He has devoted the past 25 years to the study of terrorism and international crime. After joining RAND Corporation in 1972, he planned and led government-sponsored research projects on terrorism. He later became the Director of RAND's Subnational Conflict Research Program, a position he held until his departure from the company in 1989. He also chaired RAND's Political Science Department from 1986 to 1989. He joined Kroll Associates in 1989, where his responsibilities included supervising the company's investigative and consulting work on terrorism and security. He consults with several government agencies and is currently a member of the

White House Commission on Aviation Safety and Security. His publications include *International Terrorism: A New Mode of Conflict* and *Terrorism and Personal Protection*.

**Daniel Murray** is currently Director of Technology Research at the American Trucking Associations (ATA) Foundation. The ATA Foundation is sponsored by ATA to research and develop technologies that can be used to improve trucking and highway safety, security, and productivity. His areas of expertise are freight mobility and transportation planning, and his current research focuses on the development of national intelligent transportation systems (ITS) to enhance freight efficiency and security. He has managed several large-scale research projects for the ATA Foundation, including the O'Hare International Airport Air Cargo Security Access System Project, the Multimodal Electronic Supply Chain Manifest field test, and the Tacoma–Chicago Intermodal Data Transfer Study. Prior to his current position, he was a policy analyst for ATA. He is currently a member of the Minnesota Guidestar ITS Board and the Midwest Transportation Alliance, and he served as Vice Chairman of the Minnesota Freight Stakeholders Coalition.

**Edmond L. Soliday** recently retired as Vice President for Corporate Safety, Quality Assurance, and Security at United Airlines. In this position, he directed the airline's flight safety, occupational safety, environmental safety, corporate emergency response, and corporate security programs. Serving for 11 years, he played a key role in developing many innovative flight safety programs in the aviation industry, including flight operations quality assurance, enhanced ground proximity warning systems, the Aviation Safety Action Program, and the Crew/Leadership/Resource Management Program for flight officers. He cochairs the Commercial Aviation Safety Team, an industry group that works with FAA to address significant safety issues. He is also a member of ATA's Safety Council and the Flight Safety Foundation's Executive Committee. He worked for United for more than 35 years and was a Boeing 767 captain before becoming head of corporate safety.

**Richard A. White** is General Manager and Chief Executive Officer of the Washington Metropolitan Area Transit Authority (WMATA), the regional operator of rapid transit and bus services in the greater Washington, D.C., metropolitan area. He has been General Manager of WMATA since 1996. Prior to joining WMATA, he served in several staff executive positions, including Deputy General Manager and then General Manager of the San Francisco Bay Area Rapid Transit District (BART), where he was Chief Executive Officer for the regional rapid transit and express bus service. Before joining BART, he worked with the New Jersey Transit Corporation, where he managed a variety of activities for this statewide public transportation authority. He serves on the Board of Directors of the Metropolitan Washington Council of Governments Transportation Planning Board and is Chairman of the American Public Transportation Association's Security Task Force.

**James A. Wilding** is President and Chief Executive Officer of the Metropolitan Washington Airports Authority, which operates both Ronald Reagan Washington National Airport and Dulles International Airport. He joined FAA in 1959 to participate in the original planning and development of Dulles Airport. He served as Chief Engineer for the airport until 1975, when he was appointed Deputy Director. In 1979, he was appointed Director of FAA's Washington Airports organization, which was transferred to the independent airports authority in 1987. He has served as Chairman of the Airports Council International–North America and on the board of directors of the regional organization and its parent organization in Geneva. He was a member of the TRB Executive Committee from January 1999 to January 2002.