PB2003-100209

# TCRP REPORT 86

TRANSIT COOPERATIVE RESEARCH PROGRAM

Sponsored by the Federal Transit Administration

*Public Transportation Security: Volume 1*

# Communication of Threats: A Guide

TRANSPORTATION RESEARCH BOARD

NATIONAL RESEARCH COUNCIL

**TCRP OVERSIGHT AND PROJECT SELECTION COMMITTEE**
(as of June 2002)

**CHAIR**
LINDA S. WATSON
*Corpus Christi RTA*

**MEMBERS**
DANNY ALVAREZ
*Miami-Dade Transit Agency*
KAREN ANTION
*Karen Antion Consulting*
GORDON AOYAGI
*Montgomery County Government*
JEAN PAUL BAILLY
*Union Internationale des Transports Publics*
J. BARRY BARKER
*Transit Authority of River City*
RONALD L. BARNES
*Central Ohio Transit Authority*
LINDA J. BOHLINGER
*HNTB Corp.*
ANDREW BONDS, JR.
*Parsons Transportation Group, Inc.*
JENNIFER L. DORN
*FTA*
NATHANIEL P. FORD, SR.
*Metropolitan Atlanta RTA*
CONSTANCE GARBER
*York County Community Action Corp.*
FRED M. GILLIAM
*Capital Metropolitan Transportation Authority*
SHARON GREENE
*Sharon Greene & Associates*
KATHERINE M. HUNTER-ZAWORSKI
*Oregon State University*
ROBERT H. IRWIN
*British Columbia Transit*
JOYCE HOBSON JOHNSON
*North Carolina A&T State University*
CELIA G. KUPERSMITH
*Golden Gate Bridge, Highway and Transportation District*
PAUL J. LARROUSSE
*National Transit Institute*
DAVID A. LEE
*Connecticut Transit*
CLARENCE W. MARSELLA
*Denver Regional Transportation District*
STEPHANIE L. PINSON
*Gilbert Tweed Associates, Inc.*
ROBERT H. PRINCE, JR.
*DMJM+HARRIS*
JEFFERY M. ROSENBERG
*Amalgamated Transit Union*
RICHARD J. SIMONETTA
*pbConsult*
PAUL P. SKOUTELAS
*Port Authority of Allegheny County*
PAUL A. TOLIVER
*King County Metro*

**EX OFFICIO MEMBERS**
WILLIAM W. MILLAR
*APTA*
MARY E. PETERS
*FHWA*
JOHN C. HORSLEY
*AASHTO*
ROBERT E. SKINNER, JR.
*TRB*

**TDC EXECUTIVE DIRECTOR**
LOUIS F. SANDERS
*APTA*

**SECRETARY**
ROBERT J. REILLY
*TRB*

**TRANSPORTATION RESEARCH BOARD EXECUTIVE COMMITTEE 2002 (Membership as of July 2002)**

**OFFICERS**

**Chair:** *E. Dean Carlson, Secretary of Transportation, Kansas DOT*
**Vice Chair:** *Genevieve Giuliano, Professor, School of Policy, Planning, and Development, USC, Los Angeles*
**Executive Director:** *Robert E. Skinner, Jr., Transportation Research Board*

**MEMBERS**

WILLIAM D. ANKNER, *Director, Rhode Island DOT*
THOMAS F. BARRY, JR., *Secretary of Transportation, Florida DOT*
MICHAEL W. BEHRENS, *Executive Director, Texas DOT*
JACK E. BUFFINGTON, *Associate Director and Research Professor, Mack-Blackwell National Rural Transportation Study Center, University of Arkansas*
SARAH C. CAMPBELL, *President, TransManagement, Inc., Washington, DC*
JOANNE F. CASEY, *President, Intermodal Association of North America*
JAMES C. CODELL III, *Secretary, Kentucky Transportation Cabinet*
JOHN L. CRAIG, *Director, Nebraska Department of Roads*
ROBERT A. FROSCH, *Sr. Research Fellow, John F. Kennedy School of Government, Harvard University*
SUSAN HANSON, *Landry University Prof. of Geography, Graduate School of Geography, Clark University*
LESTER A. HOEL, *L. A. Lacy Distinguished Professor, Depart. of Civil Engineering, University of Virginia*
RONALD F. KIRBY, *Director of Transportation Planning, Metropolitan Washington Council of Governments*
H. THOMAS KORNEGAY, *Exec. Dir., Port of Houston Authority*
BRADLEY L. MALLORY, *Secretary of Transportation, Pennsylvania DOT*
MICHAEL D. MEYER, *Professor, School of Civil and Environmental Engineering, Georgia Institute of Technology*
JEFF P. MORALES, *Director of Transportation, California DOT*
DAVID PLAVIN, *President, Airports Council International, Washington, DC*
JOHN REBENSDORF, *Vice Pres., Network and Service Planning, Union Pacific Railroad Co., Omaha, NE*
CATHERINE L. ROSS, *Executive Director, Georgia Regional Transportation Agency*
JOHN M. SAMUELS, *Sr. Vice Pres.-Operations Planning & Support, Norfolk Southern Corporation, Norfolk, VA*
PAUL P. SKOUTELAS, *CEO, Port Authority of Allegheny County, Pittsburgh, PA*
MICHAEL S. TOWNES, *Exec. Dir., Transportation District Commission of Hampton Roads, Hampton, VA*
MARTIN WACHS, *Director, Institute of Transportation Studies, University of California at Berkeley*
MICHAEL W. WICKHAM, *Chairman and CEO, Roadway Express, Inc., Akron, OH*
M. GORDON WOLMAN, *Prof. of Geography and Environmental Engineering, The Johns Hopkins University*

**EX OFFICIO MEMBERS**

MIKE ACOTT, *President, National Asphalt Pavement Association*
REBECCA M. BREWSTER, *President and CEO, American Transportation Research Institute, Atlanta, GA*
JOSEPH M. CLAPP, *Federal Motor Carrier Safety Administrator, U.S.DOT*
THOMAS H. COLLINS (Adm., U.S. Coast Guard), *Commandant, U.S. Coast Guard*
JENNIFER L. DORN, *Federal Transit Administrator, U.S.DOT*
ELLEN G. ENGLEMAN, *Research and Special Programs Administrator, U.S.DOT*
ROBERT B. FLOWERS (Lt. Gen., U.S. Army), *Chief of Engineers and Commander, U.S. Army Corps of Engineers*
HAROLD K. FORSEN, *Foreign Secretary, National Academy of Engineering*
JANE F. GARVEY, *Federal Aviation Administrator, U.S.DOT*
EDWARD R. HAMBERGER, *President and CEO, Association of American Railroads*
JOHN C. HORSLEY, *Exec. Dir., American Association of State Highway and Transportation Officials*
MICHAEL P. JACKSON, *Deputy Secretary of Transportation, U.S.DOT*
ROBERT S. KIRK, *Director, Office of Advanced Automotive Technologies, U.S. DOE*
WILLIAM W. MILLAR, *President, American Public Transportation Association*
MARGO T. OGE, *Director, Office of Transportation and Air Quality, U.S. EPA*
MARY E. PETERS, *Federal Highway Administrator, U.S.DOT*
JEFFREY W. RUNGE, *National Highway Traffic Safety Administrator, U.S.DOT*
JON A. RUTTER, *Federal Railroad Administrator, U.S.DOT*
WILLIAM G. SCHUBERT, *Maritime Administrator, U.S.DOT*
ASHISH K. SEN, *Director, Bureau of Transportation Statistics, U.S.DOT*
ROBERT A. VENEZIA, *Earth Sciences Applications Specialist, National Aeronautics and Space Administration*

**TRANSIT COOPERATIVE RESEARCH PROGRAM**

*Transportation Research Board Executive Committee Subcommittee for TCRP*
E. DEAN CARLSON, *Kansas DOT* (Chair)
JENNIFER L. DORN, *Federal Transit Administration, U.S.DOT*
GENEVIEVE GIULIANO, *University of Southern California, Los Angeles*
LESTER A. HOEL, *University of Virginia*
WILLIAM W. MILLAR, *American Public Transportation Association*
JOHN M. SAMUELS, *Norfolk Southern Corporation, Norfolk, VA*
ROBERT E. SKINNER, JR., *Transportation Research Board*
PAUL P. SKOUTELAS, *Port Authority of Allegheny County, Pittsburgh, PA*
MICHAEL S. TOWNES, *Transportation District Commission of Hampton Roads, Hampton, VA*

TRANSIT COOPERATIVE RESEARCH PROGRAM

# TCRP REPORT 86

## *Public Transportation Security:*

## *Volume 1*

# Communication of Threats: A Guide


JOHN N. BALOG
McCormick, Taylor & Associates, Inc.
Philadelphia, PA

MATTHEW G. DEVOST
Technical Defense, Inc.
Burke, VA

and

JOHN P. SULLIVAN
Rowland Heights, CA



Reproduced from
best available copy.

*PROTECTED UNDER INTERNATIONAL COPYRIGHT*
*ALL RIGHTS RESERVED*
NATIONAL TECHNICAL INFORMATION SERVICE
U.S. DEPARTMENT OF COMMERCE


SUBJECT AREAS
Public Transit • Planning and Administration


Research Sponsored by the Federal Transit Administration in Cooperation with the Transit Development Corporation

TRANSPORTATION RESEARCH BOARD — NATIONAL RESEARCH COUNCIL

NATIONAL ACADEMY PRESS
WASHINGTON, D.C. — 2002



NTIS
REPRODUCED BY:
U.S. Department of Commerce
National Technical Information Service
Springfield, Virginia 22161

## TRANSIT COOPERATIVE RESEARCH PROGRAM

The nation's growth and the need to meet mobility, environmental, and energy objectives place demands on public transit systems. Current systems, some of which are old and in need of upgrading, must expand service area, increase service frequency, and improve efficiency to serve these demands. Research is necessary to solve operating problems, to adapt appropriate new technologies from other industries, and to introduce innovations into the transit industry. The Transit Cooperative Research Program (TCRP) serves as one of the principal means by which the transit industry can develop innovative near-term solutions to meet demands placed on it.

The need for TCRP was originally identified in *TRB Special Report 213—Research for Public Transit: New Directions,* published in 1987 and based on a study sponsored by the Urban Mass Transportation Administration—now the Federal Transit Administration (FTA). A report by the American Public Transportation Association (APTA), *Transportation 2000*, also recognized the need for local, problem-solving research. TCRP, modeled after the longstanding and successful National Cooperative Highway Research Program, undertakes research and other technical activities in response to the needs of transit service providers. The scope of TCRP includes a variety of transit research fields including planning, service configuration, equipment, facilities, operations, human resources, maintenance, policy, and administrative practices.

TCRP was established under FTA sponsorship in July 1992. Proposed by the U.S. Department of Transportation, TCRP was authorized as part of the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). On May 13, 1992, a memorandum agreement outlining TCRP operating procedures was executed by the three cooperating organizations: FTA, the National Academies, acting through the Transportation Research Board (TRB); and the Transit Development Corporation, Inc. (TDC), a nonprofit educational and research organization established by APTA. TDC is responsible for forming the independent governing board, designated as the TCRP Oversight and Project Selection (TOPS) Committee.

Research problem statements for TCRP are solicited periodically but may be submitted to TRB by anyone at any time. It is the responsibility of the TOPS Committee to formulate the research program by identifying the highest priority projects. As part of the evaluation, the TOPS Committee defines funding levels and expected products.

Once selected, each project is assigned to an expert panel, appointed by the Transportation Research Board. The panels prepare project statements (requests for proposals), select contractors, and provide technical guidance and counsel throughout the life of the project. The process for developing research problem statements and selecting research agencies has been used by TRB in managing cooperative research programs since 1962. As in other TRB activities, TCRP project panels serve voluntarily without compensation.

Because research cannot have the desired impact if products fail to reach the intended audience, special emphasis is placed on disseminating TCRP results to the intended end users of the research: transit agencies, service providers, and suppliers. TRB provides a series of research reports, syntheses of transit practice, and other supporting material developed by TCRP research. APTA will arrange for workshops, training aids, field visits, and other activities to ensure that results are implemented by urban and rural transit industry practitioners.

The TCRP provides a forum where transit agencies can cooperatively address common operational problems. The TCRP results support and complement other ongoing transit research and training programs.

## TCRP REPORT 86: Volume 1

Project J-10B(4) FY'02
ISSN 1073-4872
ISBN 0-309-06760-X
Library of Congress Control Number 2002109708

© 2002 Transportation Research Board

**Price $15.00**

### NOTICE

The project that is the subject of this report was a part of the Transit Cooperative Research Program conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council. Such approval reflects the Governing Board's judgment that the project concerned is appropriate with respect to both the purposes and resources of the National Research Council.

The members of the technical advisory panel selected to monitor this project and to review this report were chosen for recognized scholarly competence and with due consideration for the balance of disciplines appropriate to the project. The opinions and conclusions expressed or implied are those of the research agency that performed the research, and while they have been accepted as appropriate by the technical panel, they are not necessarily those of the Transportation Research Board, the National Research Council, the Transit Development Corporation, or the Federal Transit Administration of the U.S. Department of Transportation.

Each report is reviewed and accepted for publication by the technical panel according to procedures established and monitored by the Transportation Research Board Executive Committee and the Governing Board of the National Research Council.

To save time and money in disseminating the research findings, the report is essentially the original text as submitted by the research agency. This report has not been edited by TRB.

### Special Notice

The Transportation Research Board, the National Research Council, the Transit Development Corporation, and the Federal Transit Administration (sponsor of the Transit Cooperative Research Program) do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the clarity and completeness of the project reporting.

*Published reports of the*

**TRANSIT COOPERATIVE RESEARCH PROGRAM**

*are available from:*

Transportation Research Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

and can be ordered through the Internet at
http://www.national-academies.org/trb/bookstore

Printed in the United States of America

# FOREWORD

*By S. A. Parker*
*Staff Officer*
*Transportation Research Board*

Rapid and accurate information sharing is a critical operational need for coping with threats against public transportation systems. This first volume of *TCRP Report 86: Public Transportation Security* will be of interest to transit general managers, police and staff in security, operations, communications, information technology, training, and human resources. It will also be of interest to federal, state, and local law enforcement. This volume offers information on a variety of approaches to improving the sharing of threat information. Current practices, operational needs, technologies for threat information dissemination, and system functional requirements are discussed. Effective strategies for sharing analyzed and unanalyzed reports of suspicious activities and a path to an interoperable set of national, regional, and local threat-information forums are proposed. This volume was prepared by McCormick, Taylor & Associates, Inc., under TCRP Project J-10B(4).

---

Emergencies arising from terrorist threats highlight the need for transportation managers to minimize the vulnerability of passengers, employees, and physical assets through incident prevention, preparedness, response, and recovery. Managers are seeking to reduce the chances that transportation vehicles and facilities will be targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. By being prepared to respond to terrorism, each public transportation agency is simultaneously prepared to respond to natural disasters such as hurricanes, floods, and wildfires, as well as human-caused events such as hazardous materials spills and other incidents. In the last week of October 2001, the Transit Cooperative Research Program budgeted $2 million for security-related research in fiscal year 2002.

This is the first volume of *TCRP Report 86: Public Transportation Security,* a series in which relevant information is assembled into single, concise volumes, each pertaining to a specific security problem and closely related issues. These volumes will focus on the concerns that transit agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the report will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including a number of public transportation agencies. A topic panel of experts in the subject area was established to guide the researchers in organizing and evaluating the collected data and to review the final document.

This volume was prepared to meet an urgent need for information in this area. It records practices that were acceptable within the limitations of the knowledge available at the time of its preparation. Work in this area is proceeding swiftly, and readers are encouraged to be on the lookout for the most up-to-date information.

Volumes issued under *TCRP Report 86: Public Transportation Security* may be found on the TRB website at http://www4.trb.org/trb/crp.nsf/All+Projects/TCRP+J-10.

TABLE OF CONTENTS


| SECTION | PAGE |
|---|---|
| INTRODUCTION | 1 |
| CURRENT PRACTICE AND OPERATIONAL NEEDS | 3 |
| COMMUNICATION OF THREATS SURVEY | 5 |
| SURVEY: BACKGROUND INFORMATION | 6 |
| SURVEY: ASSESSMENT OF CURRENT PRACTICES | 6 |
| SURVEY: ASSESSMENT OF OPERATIONAL NEEDS AND PREFERENCES | 8 |
| SYSTEM DESIGN | 9 |
| INTEROPERABILITY | 9 |
| INFORMATION SURETY (OPERATIONAL SECURITY) | 9 |
| WHAT LEVEL OF SECURITY | 10 |
| CURRENT INFORMATION SHARING MECHANISMS | 10 |
| THREAT INFORMATION NEEDS | 10 |
| COMMENTS/SUGGESTIONS FOR IMPROVED COMMUNICATION OF THREATS | 11 |
| SURVEY: SUMMARY AND CONCLUSIONS | 11 |
| ASSESSMENT OF CURRENT PRACTICES | 11 |
| ASSESSMENT OF OPERATIONAL NEEDS AND PREFERENCES | 11 |
| OPERATIONAL PARAMETERS: THREAT INFORMATION FORUM | 12 |
| TECHNOLOGIES FOR THREAT INFORMATION DISSEMINATION | 14 |
| SYSTEM FUNCTIONAL REQUIREMENTS | 15 |
| SCALABLE INFRASTRUCTURE DESIGN | 15 |
| DATABASE STORAGE | 16 |
| MULTI-LEVEL AND MULTI-TYPE INPUT MECHANISMS | 16 |
| MULTIPLE DISSEMINATION MECHANISMS | 17 |
| MESSAGE CONTENT | 18 |
| SUPPLEMENTAL ISSUES | 18 |
| CONCLUSION | 18 |
| REFERENCES | 20 |
| APPENDIX A: ACRONYM LIST | 21 |
| APPENDIX B: PUBLIC TRANSPORTATION SYSTEMS PERSONNEL SENT SURVEY RESEARCH INSTRUMENTS | 23 |
| APPENDIX C: SURVEY INSTRUMENT AND TRANSMITTAL LETTER | 27 |
| APPENDIX D: HOMELAND SECURITY ADVISORY SYSTEM (HSAS) CONDITIONS | 33 |
| APPENDIX E: PROPOSED NEXT STEPS | 35 |
| APPENDIX F: SURVEY RESULTS | 37 |


Preceding Page Blank

## COOPERATIVE RESEARCH PROGRAMS STAFF FOR TCRP REPORT 86

ROBERT J. REILLY, *Director, Cooperative Research Programs*
CHRISTOPHER JENKS, *TCRP Manager*
S. A. PARKER, *Senior Program Officer*
EILEEN P. DELANEY, *Managing Editor*
ELLEN M. CHAFEE, *Assistant Editor*

## TCRP PROJECT J-10B PANEL
### Field of Special Projects—Area of Security

BARRY J. McDEVITT, *Washington Metropolitan Area Transit Authority* (Chair)
WILLIAM J. FLEMING, *Massachusetts Bay Transportation Authority*
ERNEST R. "RON" FRAZIER, *AMTRAK, Wilmington, DE*
BEN GOMEZ, *Dallas Area Rapid Transit*
JOSEPH E. HOFMANN, *Metropolitan Transportation Authority–New York City Transit*
JOHN K. JOYCE, *Greater Cleveland Regional Transit Authority*
DANIEL KEYES, *University of Texas, Southwestern Medical Center, Dallas, TX*
K. SCOTT KIMERER, *King County Sheriff/Metro Transit Police, WA*
LISA A. MANCINI, *San Francisco Municipal Railway*
FRANK T. MARTIN, *Santa Clara Valley Transportation, CA*
MICHAEL J. WALKER, *Toronto Transit Commission*
PATRICIA WEAVER, *University of Kansas*
RICHARD WINSTON, *Chicago Transit Authority*
LEONARD E. DIAMOND, *FTA Liaison Representative*
QUON KWAN, *FTA Liaison Representative*
TERRELL WILLIAMS, *FTA Liaison Representative*
GREG HULL, *APTA Liaison Representative*
VIVIENNE WILLIAMS, *APTA Liaison Representative*
ALLAN J. DeBLASIO, *Volpe National Transportation Systems Center Liaison Representative*
PAUL GOLDEN, *National Infrastructure Protection Center Liaison Representative*
CHRISTOPHER A. KOZUB, *National Transit Institute Liaison Representative*
LENA TIMMONS, *Easter Seals Project ACTION Liaison Representative*
JOEDY W. CAMBRIDGE, *TRB Liaison Representative*
PETER SHAW, *TRB Liaison Representative*

## INTRODUCTION

The operational world of public transportation is complex and multifaceted. Public transportation systems in the United States include automated guideway, rail, bus, ferry and paratransit modes. Public transportation is a critical subset of the national transportation infrastructure and a major component of the economy. Surety of public transportation is largely reliant on the ability to rapidly and accurately identify and communicate threats against its passengers, employees, vehicles, and facilities. A series of working protocols for identifying and disseminating threat information to and among public transportation operators, security personnel, and law enforcement agencies to facilitate threat identification, response, and mitigation activities is presented. Included is a summary assessment of current practices and operational needs within the public transportation community, along with a suggested framework for an improved system.

Threat identification and dissemination is an essential element of homeland security. Whereas large-scale or otherwise significant attacks (both in terms of duration and scope) place public transportation infrastructure and national security at risk, even short-term disruptions can have significant operational, psychological (in terms of public and employee confidence), and/or economic impact. Devastation can extend to other vital sectors of the nation's critical infrastructure. Public transportation systems are interdependent with other critical infrastructures (especially the communications and information sectors), and the impact of an incident or event during service provision can have cascading effects because of the complexity and resulting multi-sector vulnerability. For example, most commuters use just-in-time arrival goals in planning their work trips. They know when they are required to be at work and take scheduled public transportation vehicles that will allow for on-time arrival. A serious incident involving the public transportation infrastructure would cause large numbers of employees to be late to work or to not arrive at work at all. This impact is reinforced, as their non-productivity would cause similar economic impacts to commerce partners.

Public transportation systems (passenger rail including subways, metros, light rail, commuter, and interurban rail) and transportation terminals (bus, rail, ferry, intermodal) are vulnerable to terrorist attacks such as a disruption to the transportation infrastructure, which includes various types of terrorism and sabotage. Disruptions directed towards public transportation systems can place communities and national security at risk. Significant economic losses and interruption of vital services are also a result of terrorist attacks. Public transportation is also susceptible to secondary impact from attacks directed against the energy, communications, and information infrastructures, as well as attacks on public facilities [e.g., the first and second World Trade Center attacks resulted in significant impact on the Port Authority Trans Hudson (PATH) and New York City (NYC) Subway systems].

Public transportation systems are vulnerable to attack or intentional disruption for a number of reasons[1]. Characteristics contributing to the vulnerability of public transport include:

- carrying a large number of people within enclosed spaces;
- following known or fixed routes during a predictable timeframe;
- having fixed access points;
- containing unique hazards (e.g., traction power, confined spaces, etc.) that complicate response; and
- being susceptible to systemic impacts.

Attacks against transport targets can be directed at casualty generation, disruption or both. Recent attacks targeting transport systems (by terrorists or criminal actors) include the 1994 Fulton Street firebombing on the NYC Subway, the derailment of the Amtrak Sunset Limited in Hyder, Arizona in 1995, the 1993 Long Island Rail Road (LIRR) shooting, the 1995 Tokyo Sarin attack by Aum Shinrikyo, the 1995-96 bombing campaign against the Paris Metro by the Groupe Islamique Arm (GIA), armed Islamic group, and the 1997 plot to bomb the Atlantic Avenue subway and Long Island Railroad (LIRR) station in Brooklyn. Ongoing attacks directed against Israeli buses and recent intelligence information (FBI and DOT advisories and alerts) regarding al-Qaeda interest in attacking US subways and employing chemical agents, combined with attempts to acquire chemical/biological/radiological/nuclear (CBRN) means to reinforce the viability of terrorist threats against public transportation. Attacks against public transportation systems or infrastructure can have significant impact in terms of lives and system status. Responding to such attacks will necessitate good intelligence and significant demands for information by decision makers and emergency responders. The presence of an opposing will, time constraints, and incomplete or conflicting information can be expected to complicate response, mitigation, and the decision-making process.

The transportation infrastructure, at its largest extent, includes a combination of privately and publicly held passenger and freight assets that should be addressed in totality. However, the public transportation sector is the only concern of this report. Public transportation systems include the guideways and roadways on which the various vehicles operate, the administrative, control, and maintenance facilities that support service provision, the passengers who ride the system, the employees who facilitate operation, and the Public Transportation Information Infrastructure (PTII)[2]. The PTII consists of transportation data, software, hardware, and communication technology.

---

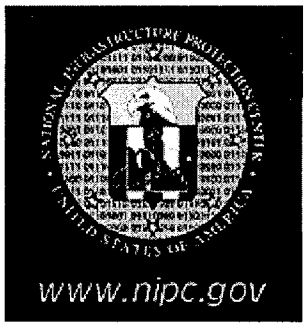
[1] See "Terrorism and Attacks Against Transit Systems" in "Chapter VI: Transportation Systems," Kozlow, Christopher and Sullivan, John, *Jane's Facility Security Handbook*, Jane's Information Group, Alexandria, VA, 2000 and Boyd, Annabelle and Sullivan, John P., *Emergency Preparedness for Transit Terrorism*, TCRP Synthesis 27, Transportation Research Board, Washington, DC, 1997 for additional information on threats to transportation systems.

[2] A number of acronyms are used in this report. They are defined in Appendix A.

The threat communication (identification and dissemination) mechanism described herein would form a critical component of the PTII as well as serve as a means of protecting the PTII and identifying threats against it and the public transportation infrastructure. In surface transportation, the emerging Intelligent Transportation System (ITS) component is another important element of the PTII.

A viable public transportation threat communication mechanism should be an integral component of an overarching, industry-wide consequence management architecture and provide for information surety.

Threat identification, threat management, and consequence mitigation are three elements of a robust approach to crisis management. All rely upon good information flow and the rapid identification and dissemination of threat knowledge and situational awareness to all potentially affected public transportation system operators, intelligence organizations, and law enforcement authorities, whereas maintaining a link with other infrastructure sectors [directly or through a collaborative threat information forum (TIF) such as InfraGard[3]]. Information surety is a measure of the integrity, confidentiality, and accessibility of information and must be incorporated into this effort.




## CURRENT PRACTICE AND OPERATIONAL NEEDS

Public transportation operators and security components (including sworn public transportation officers and local municipal police) currently receive threat and intelligence information from a variety of formal and informal sources. These include:

- advisories from the United States Department of Transportation (USDOT) [including information from the Federal Transit Administration (FTA) and the Transportation Security Administration (TSA)];
- advisories from the FBI's InfraGard program;
- notifications from local law enforcement and emergency management agencies; and
- news reportage (open source intelligence).

---

[3] The InfraGard Program is an essential component of the National Infrastructure Protection Center (NIPC) that conducts outreach and information sharing with the public and private sector owners and operators of critical infrastructures. The program establishes a mechanism for two-way information sharing about intrusion incidents and system vulnerabilities and provides a channel for the NIPC to disseminate analytical threat products to the private sector. The mission of the NIPC is to detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies, both physical and cyber, that threaten or target critical infrastructures; manage computer intrusion investigations; support law enforcement, counterterrorism, and foreign counterintelligence missions related to cyber crimes and intrusion; support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and coordinate training for cyber investigators and infrastructure protectors in the government and private sector.

Direct reports from employees or customers are also key sources of threat information. Often in the form of an alert, threat information is disseminated (though, not often formally) through a number of delivery systems (email, fax, surface mail, telephone, etc.) and varies in timeliness, accuracy, and utility value.

Threat identification is absolutely necessary for recognizing a potential attack targeting a specific public transportation system. Certain trends, as shown in Figure 1, may serve as an early warning system to a possible security threat. Recognition of these trends may even prevent a coordinated attack against multiple public transportation systems, if discovered in time and communicated effectively to the other systems.

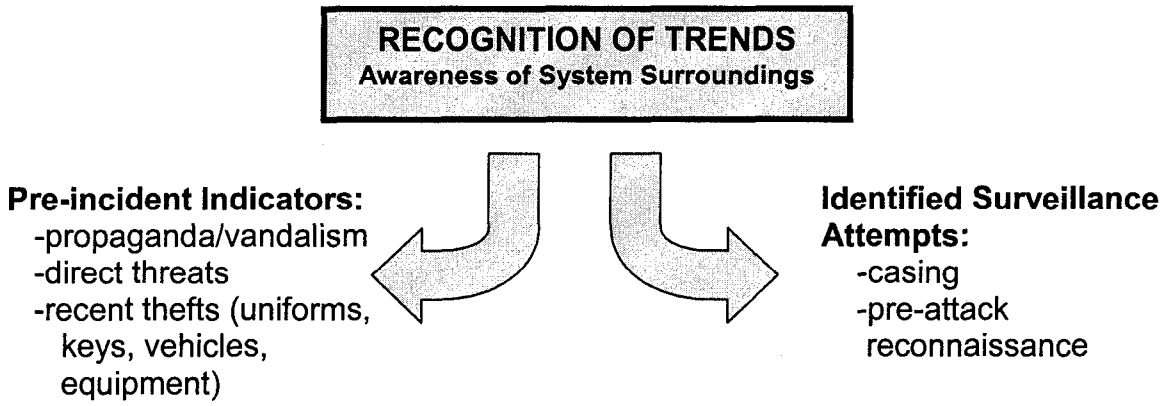



**FIGURE 1: RECOGNITION OF TRENDS**

Awareness of current threat situations allows public transportation systems to allocate resources for security and counterterrorism efforts and to identify operational and security posture (such as measures to deter and prevent, or rapidly assess and mitigate an incident). This general awareness keeps decision makers informed so they can decide on whether to initiate any of the following actions:

- ❒ suspending or restricting service;
- ❒ alerting the public of possible threats;
- ❒ implementing patron security measures (such as reporting suspicious persons or packages); and/or
- ❒ conducting employee awareness briefings.

Historically, public transportation systems have shared threat information with varying levels of effectiveness. For example, public transportation systems (or public transportation police forces) were previously surveyed in another Transit Cooperative Research Program (TCRP) project.[4] It was established that 55% maintained regular links with other public transportation systems regarding threat posture and 71%

[4] Boyd, Annabelle and Sullivan, John P., *Emergency Preparedness for Transit Terrorism, TCRP Synthesis 27*, Transportation Research Board, Washington, DC, 1997.

maintained on-going links with local, state, or federal law enforcement agencies with the specific intent of maintaining awareness of current threat. These are strong and positive levels of interaction. However, in today's post September 11 environment, it is suggested that every public transportation and paratransit system establish a strong working relationship with other public transportation systems in their region (and beyond); with private bus operators and other transportation providers (such as school bus operators); and with local, state, and federal law enforcement agencies.

Additionally, whereas 93% of respondent systems received threat/warning circulars from the FTA or USDOT/Office of Intelligence and Security (OIS), dissemination to key personnel at the managerial and operational levels was much lower, as shown in Figure 2. This is not very reassuring, because the information received was not always communicated to the rank and file operations personnel who would have needed to take definitive action if warranted.

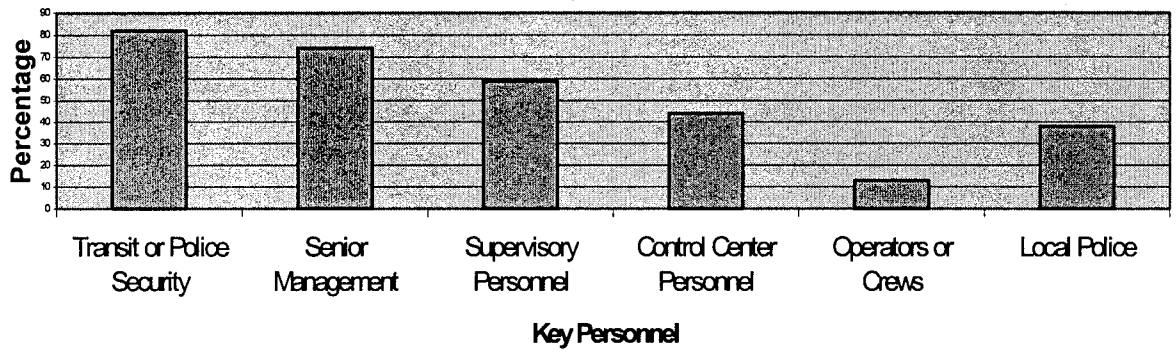



**FIGURE 2: PERCENTAGE OF TRANSIT SYSTEM KEY PERSONNEL WHO RECEIVED THREAT OR WARNING CIRCULARS FROM THE FTA OR USDOT/OIS.**

## COMMUNICATION OF THREATS SURVEY

As a component of the research associated with this Communication of Threats program, in April 2002, a survey instrument was generated and distributed to 39 public transportation systems[5] to determine the current sources of threat information they receive and the delivery mechanisms that would facilitate interaction with the technology currently deployed within their organization. From a total of 39 surveys sent, the MTA research team received responses from 12 transportation authorities including, Chicago, Cleveland, Dallas, Denver, Kenosha, WI, Miami, North Carolina, Northern Indiana, Sacramento, San Francisco, Washington, DC, and Utah.

[5] The public transportation systems included in the survey are listed in Appendix B. It was part of the research methodology to survey the larger systems, because they tended to have security departments or a sworn police force as a major part of the public transportation system. The survey instrument and the transmittal letter are reproduced in Appendix C. The detailed survey results are located in Appendix F.

## SURVEY: BACKGROUND INFORMATION

Nearly all respondents (10) manage bus networks, whereas almost an equal number (9) coordinate paratransit and light rail systems. Only half of the respondents (six) manage their own police departments, whereas the remaining respondents supervise their own security system.

The MTA research team attempted to gather information on both the number of threat warnings as well as the anticipated threat incidents each year from 1998 to 2001. The terms *Threat Warning* and *Actual Threat Incidents* were confusing to many respondents. The few that reported on these events tended to focus the meaning to bomb threats (this may be due to the fact that the survey was conducted by the Terrorism Research Center and thus, respondents tried to respond to threats and incidents of terrorism). Nevertheless, bomb threats have historically constituted the largest segment of concern for public transportation operators; this can be expected to continue. Furthermore, all the elements of information analysis, threat dissemination, and course of action development facing decision makers in bomb threat situations are present in more complex or exotic threats. Comparing the tables from 1998-2000, incidents outnumbered threats two to three times each year. In 2001, mostly following the heightened alert after September 11, warnings and incident responses increased dramatically. Of the 12 respondents, the total number of threats quintupled to 24 in 2001, compared with the average of 5 from 1998-2000. Additionally, the number of threat incidents to which personnel were dispatched doubled to 25 in 2001, compared with the average (12.67) from 1998-2000.

Of the 12 surveys collected, only 1 public transportation body reported more than 4 warnings in a calendar year. Interestingly, one transportation authority received approximately 15 warnings directly after September 11, 2001. No more than 10 incidents took place in any given year from 1998-2001 to which security personnel were dispatched.

## SURVEY: ASSESSMENT OF CURRENT PRACTICES

The survey assessed current public transportation threat communication practices. Specifically, the survey:

- ❒ reviewed current sources of transportation threat communications;
- ❒ explored if and how the newly developed federal Homeland Security Advisory System (HSAS) has been integrated into transportation systems;
- ❒ surveyed the timeliness and utility of a variety of threat communication media;
- ❒ investigated how public transportation system security departments currently respond to threat advisories;
- ❒ questioned if security postures are coordinated with neighboring public transportation systems; and

- ❒ derived a list of public transportation authority positions responsible for determining threat levels to the system.

Nineteen threat communications sources were presented in the questionnaire. Respondents were asked to identify which sources their public transportation system utilized as well as to rate the importance of each source on a scale of 1 (least important) to 7 (most important). Interestingly, open source news broadcasts received the highest rating of importance (average score 6.22 among 9 respondents), almost a half point higher than the next highest source. FTA received an average importance rating of 5.80 among 10 respondents. Other important sources identified by survey participants include Local Law Enforcement (5.64 score, 11 respondents), Local Emergency Management (5.50 score, 10 respondents), and Training Opportunities (5.44 score, 9 respondents). All other sources received average scores below 5.00. The lowest scoring sources surveyed include the National Crime Information Center (3.78 score, 9 respondents), Office of Intelligence and Security (3.57 score, 7 respondents), and the Federal Railroad Administration (FRA) (3.17 score, 6 respondents). Three other threat communication sources were identified including the California Anti-Terrorism Information Center (CATIC) (5 score, 1 respondent), state Office of Emergency Services (OES) (6 score, 1 respondent), and FBI Joint Terrorism Task Force (7 score, 1 respondent).

Regarding the newly developed Homeland Security Advisory System (HSAS), only half (six) of the respondents reported having been briefed about the system, and only two indicated that the HSAS had been integrated into their existing threat communication protocol. One survey participant noted that their formal threat protocol was still in development within their committee that meets twice per month to address terrorism issues. The respondent further reported that they anticipate using the HSAS threat level to determine adjustments in staffing, assignment of fixed posts at vulnerable points, etc. It should be noted that the survey was conducted approximately three months after the federal Office of Homeland Security first introduced their threat level system.

Next, the methods for threat communication, including cell phones, email, faxes, line phones, pagers/BlackBerry, and surface mail/postal service were all examined in terms of both timeliness and utility on a scale of 1 (slow/not useful) to 7 (fast/extremely useful). Line phones were identified as slightly more timely (6.17 average score) than cell phones (6.08 average score). Surface mail was described as the slowest (1.45 average score), whereas the other three media received average scores of approximately 4.5.

The survey then sought to determine if public transportation systems incorporate threat advisories into the operational status and security posture. Seven transportation networks responded positively and provided a variety of examples. Efforts listed include:

- ❒ post additional security or law enforcement personnel or secure resources based on nature of threat;

- ❒ upgrade threat status based on assessments;
- ❒ possible redeployment and increase of security personnel;
- ❒ heighten awareness of employees;
- ❒ use threat advisories to determine need for extra shifts, staffing vulnerable points, etc.;
- ❒ threat condition levels are established by standard operating procedures (general order);
- ❒ heightened state of alerts established; and
- ❒ secure critical sites.

When queried if a transport authority's security posture was subsequently coordinated with proximate or connecting public transportation systems, only two responded positively. Coordination was implemented by communicating with the police department or if asked by other systems. The surveyed public transportation authorities do appear to collect threats, but admitted little effort was made to proactively cooperate with other systems. At a minimum, this issue should be explored more and perhaps should be facilitated by future efforts.

Lastly, respondents identified the following positions as responsible for determining threat levels in their transportation systems:

- ❒ Chief of Police;
- ❒ Security Manager;
- ❒ Chief of Office of Safety and Security;
- ❒ Manager of System Security;
- ❒ President or Executive Vice President of Transit Operations;
- ❒ Director;
- ❒ Police Department Staff with advisory to District Staff; or
- ❒ currently developing threat assessment committee.

## SURVEY: ASSESSMENT OF OPERATIONAL NEEDS AND PREFERENCES

Respondents were asked to rate four components of any proposed transportation threat communication system including message vetting and authentication, peer-to-peer communication, message archiving, and historical evaluation capabilities. The first two components were rated similarly, scoring 6.09 and 6.00 averages respectively. Historical evaluation was ranked next at 4.64, whereas message archiving was rated last at 3.73.

Since the questionnaire was designed to elicit input into the design of an integrated transportation threat communication system, the research instrument collected information on the preferred media to be included. Nine respondents suggested the Internet be incorporated into the system whereas seven would like to see both cellular and pager networks included in the design. Additional suggestions included two requests for landline phones and one note to add faxed distribution. The National Criminal Information Center (NCIC) and similar state systems were also mentioned.

Most (75%) respondents did believe a Web-based system would meet their needs, although three did not. One of the three indicated that a Web-based system would not entirely meet their needs. Eight respondents supported both a public and restricted-access website design as well as tiers of access (noting full access to local law enforcement such as municipal police and sworn officers of the public transportation system). One authority recommended the website should be for law enforcement only, not for general distribution. A variety of similar password/user identification procedures were provided by respondents including:

- ❒ secure and protected/monitored;
- ❒ name and password;
- ❒ user specific alpha-numeric codes with periodic renewals; and
- ❒ encrypted.

The survey concluded by requesting a variety of suggestions on topics for design of a new integrated transportation threat communication system. Those topics and the exact responses are listed below.

**System Design**

Respondents were asked to provide comments on desirable system attributes. Examples of the responses follow.

- ❒ "Easy and fast to user."
- ❒ "Simple and redundant."
- ❒ "Constantly upgraded."
- ❒ "Our dispatch uses phone as communication tool. We will be part of combined communications system with public safety in the future. We are a small transit system and utilize our local police and fire departments as our security eyes and ears."

**Interoperability**

Respondents were asked to provide comments on system interoperability. Examples of the responses follow.

- ❒ "Allow for ease of communication and/or integration with other agencies."
- ❒ "Make available all information sharing."
- ❒ "System should be 'user-friendly' to allow easy exchange of info with source and other similar agencies."

**Information Surety (Operational Security)**

Respondents were asked to provide comments on information surety and operational security. Examples of the responses follow.

- ❒ "Restrict access based on levels of responsibility."
- ❒ "Include all public safety entities."
- ❒ "Consider use of NCIC to distribute info to law enforcement agencies in a secure mode."

**What Level of Security**

Respondents were each asked to provide comments on the desirable level of security for the system. Examples of the responses follow.

- ❒ "All levels."
- ❒ "General Information (low)."
- ❒ "Specific Information (high)."
- ❒ "All levels."
- ❒ "Prefer the availability of 'law enforcement sensitive' information."
- ❒ "Top Secret Clearance."
- ❒ "Allow select individuals at transit properties to have access similar to that maintained by law enforcement agencies."

**Current Information Sharing Mechanisms**

Respondents were asked to provide comments on current information sharing mechanisms. Examples of the responses follow.

- ❒ "Standardize bandwidth/radio frequencies/jargon, etc."
- ❒ "Email/Web access."
- ❒ "The number of sources needs to be consolidated."
- ❒ "Local law enforcement, FTA, FBI, Homeland Security National Alert System."
- ❒ "Through FBI Joint Terrorism Task Force (JTTF), Bay Area Terrorism Working Group, state OES, local contacts."
- ❒ "Phone (cell), fax machine."

**Threat Information Needs**

Respondents were asked to provide comments on threat information needs. Examples of the responses follow.

- ❒ "Assessment of threats to identify credibility."
- ❒ "Pertains to our local area, then nationwide."
- ❒ "Timely."
- ❒ "RISS [Regional Information Sharing System, a law enforcement information system sponsored by the US Department of Justice] – would be advantage to public transportation systems."
- ❒ "Needs to be timely and some measure of how reliable the information is."

## Comments/Suggestions for Improved Communication of Threats

Lastly, some sections were offered to the respondents to ask questions and provide comments to the survey administrators. One response received stated:

"Most problems I have observed in transit agencies are from systems that do not have their own police department. We have had good cooperation from local FBI office and maintain liaison with several federal and state groups."

## SURVEY: SUMMARY AND CONCLUSIONS

The survey confirmed the need for a mechanism for information sharing and threat communication for public transportation systems and related agencies.

## Assessment of Current Practices

Respondents indicated that they received threat communications from at least 22 different sources, but rated broadcast news reports as their most important source. Other highly rated sources include FTA, local law enforcement, local emergency management, and training opportunities. This reliance on local sources over traditional centralized sources (e.g., USDOT) suggests transportation operators will be slow, if not reluctant, to integrate the new HSAS. Survey results indicate that traditional phones and cell phones remain the current preferred communication methods over email/Internet and other systems. Significantly, questionnaire responses indicate little effort is made to coordinate responses among neighboring public transportation systems once threats are received. This gap should be explored further, and expanded communication should be fostered. Lastly, a review of the threat response decision makers indicates that most systems require the senior security or police official to determine operational responses and respond to threat communications.

## Assessment of Operational Needs and Preferences

Respondents emphasized tactical needs for message vetting and peer-to-peer communication, and left strategic archiving and trend analysis as lower priorities. A close examination of this section of the survey reveals that greater clarity was needed to distinguish between the communication of the threat from outside sources to the transportation system, and filtering and forwarding that threat information to vehicle operators as well as security and police personnel. Thus, it seems likely that respondents did not adequately consider the value of a Web-based network for system administrators, preferring, instead, to assess the impact of a proposed system at the individual operator levels. However, 75% of respondents fully supported the development of a web-based threat communication system.

## OPERATIONAL PARAMETERS: THREAT INFORMATION FORUM

Rapid and accurate information sharing is a critical operational need for coping with and managing threats against public transportation systems. Public transportation police, security, and operations personnel need to be aware of threats directed against their systems at the earliest opportunity. This information is essential to formulating appropriate operational responses to protect public transportation passengers, employees, vehicles, and facilities. This process is referred to as a Threat Information Forum (TIF).

It is important for public transportation threat information to simultaneously move in three directions to ensure complete and effective communication. These are:

- **top-down,** including information provided from national intelligence such as the current Homeland Security Advisory System (HSAS), which rates the status and threat to the national transportation infrastructure;

- **bottom-up,** from public transportation police, security, and operational personnel, regarding actual and suspected local threat incidents that might indicate targeting or an impending attack; and

- **lateral,** shared among adjacent public transportation systems and interrelated infrastructure sectors, representing mutual security concerns and operational issues.

In order to facilitate information sharing among all levels, a framework for a TIF, common parameters, and protocols need to be established.

TIFs should be organized into three components to collect and disseminate three classes of information. The three component areas are as follows.

- **Local public transportation threat user groups (TUGs)** should be composed of designated persons at specific public transportation systems (e.g., management, operations, security, public transportation police, control center, and other key decision makers). Local TUGs should also include designated local partners such as adjacent or cooperating public transportation systems, local police and emergency management agencies, local InfraGard chapters, and/or local threat assessment and warning entities, such as regional terrorism early warning (TEW) groups and joint terrorism task forces (JTTFs). Individual users and agency representatives should register with their TUG. Each TUG would designate a group manager and threat officer responsible for managing their local user group and disseminating information within the group. Messages could be TUG-specific or disseminated to the national clearinghouse for broader dissemination. Individual TUG users would be designated a level of access to TIF products based upon their need to know.

- **A national public transportation threat clearinghouse** should be located within an appropriate federal agency such as the USDOT's OIS, the Transportation Security Administration (TSA), the National Response Center (NRC) or the proposed Surface Transportation Information Sharing and Analysis Center (ST-ISAC)[6]. This node would be responsible for collecting, verifying, analyzing, and disseminating TIF products and messages to public transportation systems (which would be organized into TUGs), appropriate federal entities (such as the FBI and intelligence community), and other infrastructure sectors (perhaps the InfraGard program). Individual TUGs (and their designated users) would register with the national clearinghouse. This could facilitate dissemination of critical security messages to the entire forum, select TUGs, or individual users.

- **Transportation and related infrastructure owners** also need to be notified of significant threats. Key representatives of the broader transportation infrastructure and interdependent infrastructures have a need for information regarding specific crosscutting incidents and threats. It is suggested that the existing InfraGard program can be used to disseminate this information. Appropriate public transportation threat information could be disseminated from the national clearinghouse to these sectors through the network of local InfraGard chapters.

Whereas a centralized entity is required for analysis and coordination at the national level, the core component of the TIF should be the local public transportation TUGs. Any enabling technology for threat information assessment should ensure that TUGs have the capability to freely share information among themselves via mechanisms such as email, secure Web, and fax. In most cases, the requirement for rapid information sharing will require that information be shared in raw format, without vetting from a centralized analytical cell.

Individual users would be recommended and vetted by the local TUG. As an added security measure, each user would be screened through the InfraGard application and background check process, which is managed by the FBI. These measures would help ensure the integrity of the system and enhance operational security. This system should not be used for the dissemination of classified information.

The three suggested classes of information to be disseminated are advisories, alerts, and warnings. Each of these is described below.

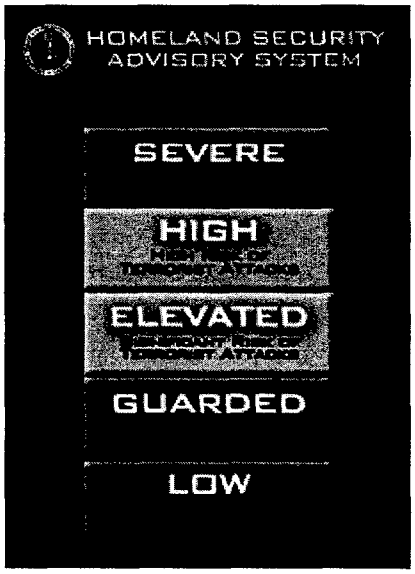
- **Advisories or incident reports** should include changes in HSAS threat status, notification of incidents (including breaking news regarding specific public transportation attacks), information on public transportation system status (restricted service, suspended service, etc.), and information regarding observed terrorist tactics, techniques, and procedures (TTPs). Advisories would be

[6] On May 2, 2002, U.S. Secretary of Transportation, Norman Y. Mineta, announced creation of the Surface Transportation Information Sharing and Analysis Center (ST-ISAC) that is designed to promote security in the transportation sector.

informal in nature and could be disseminated locally within a TUG or through the national clearinghouse to other TUGs or infrastructure sectors. Dissemination of incidents regarding suspicious circumstances would only occur after analysis and deconfliction (deconfliction is a technical process of vetting and validating a specific threat to eliminate multiple reports about the same threat) with appropriate investigative authorities to ensure operational security and avoid compromising investigative and law enforcement activities. Advisories would generally be issued during low (green) or guarded (blue) HSAS conditions. They can also relate to incident-specific information during any HSAS condition. Advisories would be disseminated to users; incident reports would originate with individual users for assessment, collection, and dissemination by a TUG or the national clearinghouse.

- **Alerts** would be threat-specific messages informing a public transportation system or TUG of a higher threat potential or to anticipate and be on the look out (BOLO) for a specific actor or threat. Alerts would generally be issued during elevated (yellow) or high (orange) HSAS conditions.

- **Warnings** would be threat-specific messages regarding an imminent threat of attack against a specific target location or venue. Warnings would only be issued during severe (red) HSAS conditions to specifically designated users within the TIF, based upon user need to know. Generally, warning messages would be disseminated as a text with direction to contact or consult a secure mode of communication or authority for specific details.




Since rapid dissemination of information is essential, it is suggested that the TIF utilize and exploit as many modes of transmission as possible. For example, an individual user should be able to receive and transmit text messages via several redundant pathways such as mobile phone, pager, two-way message unit, fax, phone, and email to ensure timely and accurate notification.

## TECHNOLOGIES FOR THREAT INFORMATION DISSEMINATION

Several commercial off-the-shelf (COTS) solutions could be assembled and customized to create a system that facilitates the exchange of threat information among public transportation systems. The suggested implementation would be to create a secure portal-like content management system that interfaces with a commercial-grade database program. This portal would be capable of collecting and disseminating threat information using multiple communication mechanisms. A notional representation of information flow is provided in Figure 3.

The portal should reside on the Internet, thereby ensuring a maximum coverage profile. However, access should be restricted to authorized personnel and protected by username or password combinations. Furthermore, users should be subjected to application and credential verifications similar to, or in coordination with, the InfraGard program.

It is suggested that the solution also provide for segmentation or enclave capabilities to allow for user communities to exchange threat information at federal, state, regional, and local levels. This would facilitate local information exchange whereas preventing information overload at the stakeholder level. These local enclaves, including TUGs, could also establish liaisons with other local or regional intelligence efforts (i.e. terrorism early warning groups) to maximize information exchange.

Notional Surface Transportation Threat Information Forum

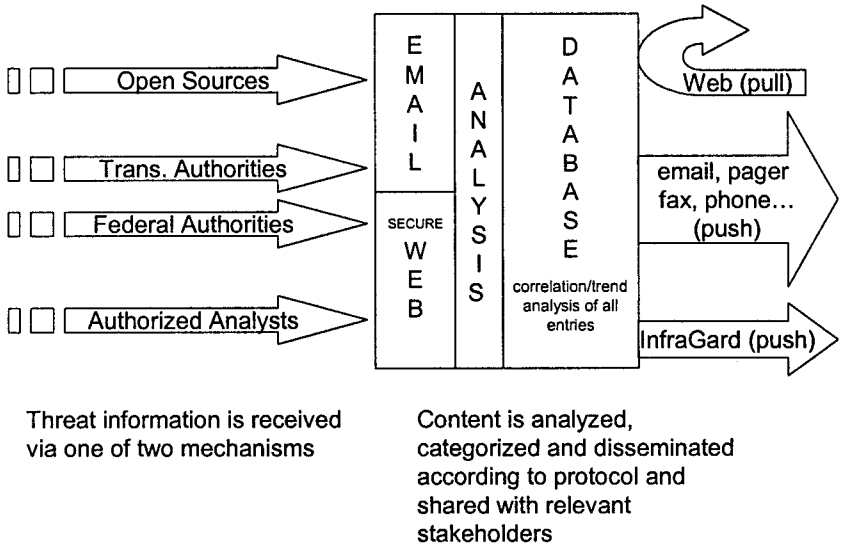



**FIGURE 3: NOTIONAL SURFACE TRANSPORTATION THREAT INFORMATION FORUM**

## SYSTEM FUNCTIONAL REQUIREMENTS

Suggestions regarding the system functional requirements for a public transportation information exchange system are presented in the subsections that follow.

### SCALABLE INFRASTRUCTURE DESIGN

The system should be designed using a scalable architecture approach that allows for the TIF portal to be implemented at a cost-effective scale and then grow as more public transportation authorities become involved. This scalable approach would also allow for smaller TIF portals to be established at the regional level that are then tied together by a centralized portal housed within an analytical center staffed to perform analysis and

facilitate information exchange at the national level. Figure 4 provides an overview of a potential distributed model.

## DATABASE STORAGE

Threat advisories, alerts, and warnings should be stored indefinitely in a commercial-grade database that allows for the interactive search and retrieval of records. Aggregating the data in one place would allow analysts to derive trends and conduct historical analysis. The system should also be capable of supporting information technology industry best practices for robustness and reliability.

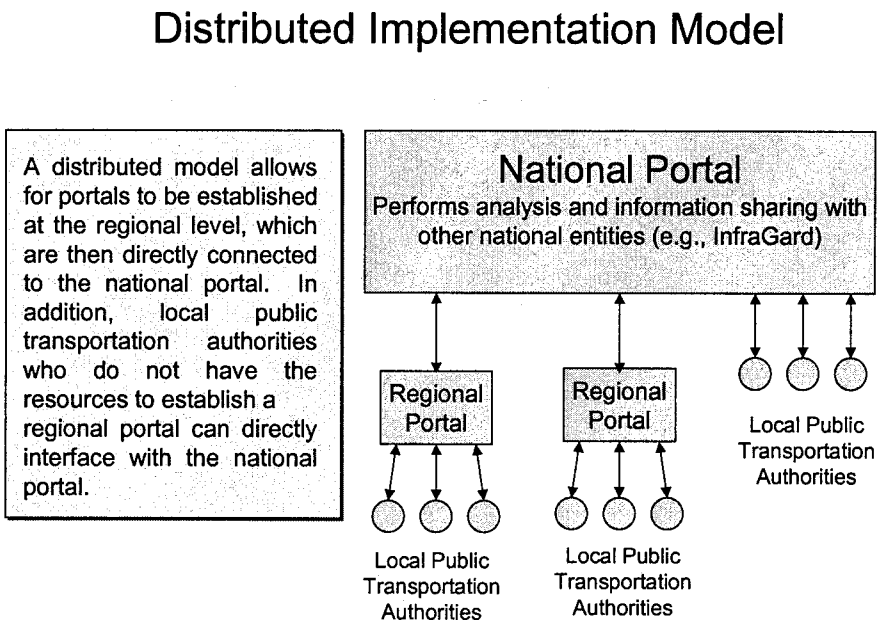



**FIGURE 4: DISTRIBUTED IMPLEMENTATION MODEL**

## MULTI-LEVEL AND MULTI-TYPE INPUT MECHANISMS

The portal should accept multiple types of information from all participating entities and categorize the information for analysis accordingly. At a minimum, input should be accepted via email and secure Web-based origins. Additionally, a Web spider capability for checking relevant websites for changes and new information would be desirable.

Support for information segregation by enclave or geographic region is suggested as is a capability for segregation of information specific to each public transportation mode (e.g., heavy rail, subway, commuter rail, light rail, rubber-tired trolley, over-the-road coach, large bus, small bus, paratransit vehicle, automated guideway public transportation vehicle, MagLev, or others).

## MULTIPLE DISSEMINATION MECHANISMS

The portal should be capable of distributing advisories, alerts, and warnings via multiple dissemination mechanisms, based on the type of information being disseminated and the established user profile. In addition, the portal should allow information to flow freely among all members of a TUG, therefore providing for real-time critical information exchange.

For maximum effectiveness, the portal should be capable of pushing information via the following interfaces.

- ❒ **Email.** The portal should be capable of sending broadcast messages to all users and also capable of sending messages to users based upon their preferred profile. For example, a user might want to receive alert and warning information to a public transportation workplace email address, and only warning messages to a personal email address. Email messages should be distributed in plain text, with all fields clearly contained within the message. In addition, messages should be digitally signed to help ensure authenticity.

- ❒ **Two-way pagers or BlackBerry[7] devices.** The portal should be capable of sending broadcast messages via two-way pager or BlackBerry devices.

- ❒ **Pagers.** The portal should be capable of sending truncated messages (within certain character lengths) to alpha-numeric pagers.

- ❒ **Facsimile.** The portal should be capable of sending broadcast fax messages (e.g., by using an Internet to fax gateway).

- ❒ **Web pull.** The portal should provide a secure Web interface allowing users to review threat information, establish their preferred communication profile, and upload threat reports to their public transportation system.

- ❒ **Telephone or mobile phone.** The portal should be capable of distributing pre-recorded messages via voice telephone communications to land and mobile telephone numbers. Given the potential associated costs, this capability would only be utilized for warning messages. Digital voice messages should also be sent.

[7] It should be understood that although BlackBerry is the name of a specific device, it is often used as a term to describe devices that are designed to wirelessly receive and send a reply to email for immediate communication and collaboration. Neither the Transit Cooperative Research Program nor the McCormick Taylor research team endorse or recommend any specific product or products.

## MESSAGE CONTENT

Each threat message (advisory or incident report, alert, or warning) would be stored in the database and disseminated based upon user profiles, geographic location, and type of message. Each message should include, at a minimum, the following data:

- originating entity;
- originating user;
- date or time of message;
- type of message (advisory/incident report, alert, warning);
- details (size, activity, location, unit, time, equipment of threat entity or actor, TTPs);
- scope of dissemination (e.g., TUG, National Infrastructure Sectors);
- dissemination restrictions (e.g., operational security considerations, no public release, public safety sensitive);
- recommended action (e.g., information only, contact specific authority, BOLO, implement security measures); and
- duration and/or expiration of threat or condition.

## SUPPLEMENTAL ISSUES

In evaluating any potential framework for the communication of threats, there are several supplemental issues that must be addressed and resolved. In addition to addressing where and how the TIF is managed, other issues surrounding legal liability and Freedom of Information Act (FOIA) responsibilities must also be researched.

It is recommended that communications be established with entities such as existing ISACs within the telecommunication and finance sectors and the FBI InfraGard administrators.

It will also be important to obtain community buy-in regarding the proposed framework and its implementation. It is recommended that a series of focus groups or workshops be conducted with representative members of the surface transportation community to drive the development of technical specifications and an implementation methodology that will help ensure the success of the proposed system. The workshops should also be used to determine the levels and types of analysis and vetting that should be performed against threat information prior to distribution. In some cases, especially among TUGs, there is a requirement for rapid dissemination that must be balanced with the requirement for vetted and accurate information.

## CONCLUSION

The communication of threats framework suggested in this discussion would establish flexible, easy-to-implement TIFs for collecting, assessing, and disseminating threats to US public transportation systems and the broader US transportation infrastructure. This framework, relying on local public transportation system enclaves, or TUGs, combined

with a national clearinghouse linked to the existing national InfraGard program, and any Information Sharing and Analysis Center (ISAC), would enable rapid, networked dissemination of threat information in a manner consistent with accepted principles of information surety.

Whereas it is important to note that technology is an enabler for rapid threat information sharing, technology should not be seen as a replacement for human analysis. To provide appropriate vetting, aggregation analysis, and coordination at both the national and local levels, a human analytical component is required. However, local public transportation authorities have a genuine requirement for rapid threat information transfer independent of a vetting or analytical process. The proposed portal concept allows for these two critical functional requirements to be met in one system. Information can be rapidly and automatically shared among TUGs, and information can be collected and analyzed to derive trends and extend information sharing outside a particular TUG as required.

One of the objectives of this research task order was to establish a framework for a communication of threats system. This has been accomplished, and the performance specifications have been initially developed. The suggested next steps to be accomplished regarding the development of the national system are more intense and summarized in Appendix E. They are presented briefly and could be further refined in the event TCRP would like to move beyond the limits of this initial effort.

This framework is dependent on the utilization of existing technology to keep costs low and ensure compatibility with existing communication capabilities within public transportation systems. The most significant costs will be associated with the development of the TIF system that ties the existing technologies together to effectively share threat information. However, if a given transportation system does not have access to the Internet, a public switched phone system for voice and fax, cellular communications, or pagers, there will be a cost of entry for the system to acquire the required technology components.[8]

---

[8] If an overall scalable architecture system were already developed and available, the cost to tie in by each public transportation system without access to existing technology at the very basic level might be $5,000. Considering that there are approximately 450 systems providing both fixed-route bus and complementary paratransit modes, as required by the Americans with Disabilities Act (ADA), and approximately 4,000 rural and community transportation systems, the approximate basic tie-in costs to the public transportation industry might be approximately $25 million. As the overall system incorporates additional capabilities and the public transportation systems increase their sophistication with respect to the level of interface with the national system, the costs would be expected to increase. The incremental costs might be $15-$25 million for each additional step beyond the basic tie-in, considering that many of the smaller rural and community transportation systems may never expand their local capability beyond the base level.

## REFERENCES

Balog, John N.; Bromley, Peter; Strongin, Jamie Beth.; Dattilio, Daniel; Boyd, Annabelle; and Caton, James, *Preliminary Draft Report: Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration, NCHRP Project 20-59(10),* National Cooperative Highway Research Program, National Academy of Sciences, Washington, DC, July 2002.

Boyd, Annabelle and Sullivan, John P., *Emergency Preparedness for Transit Terrorism, TCRP Synthesis 27*, Transportation Research Board, Washington, DC, 1997.

Government Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, Testimony Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives, Washington, DC, June 7, 2002.

Sandia National Laboratories, *US Infrastructure Assurance Strategic Roadmaps*, Section 5: US Transportation Infrastructure, SAND98-1489, August 1998, pp. 117-138.

## APPENDIX A: ACRONYM LIST

| | |
|---|---|
| ADA | Americans with Disabilities Act |
| BOLO | Be on the look out |
| COTS | Commercial off-the-shelf |
| FBI | Federal Bureau of Investigation |
| FTA | Federal Transit Administration |
| GIA | Groupe Islamique Arm (armed Islamic group) |
| HSAS | Homeland Security Advisory System |
| ISAC | Information Sharing & Analysis Center |
| ITS | Intelligent Transportation Systems |
| JTTFs | Joint Terrorism Task Forces |
| NCHRP | National Cooperative Highway Research Program |
| NIPC | National Infrastructure Protection Center |
| NRC | National Response Center |
| OES | Office of Emergency Services |
| OIS | Office of Intelligence and Security |
| PTII | Public Transportation Information Infrastructure |
| ST-ISAC | Surface Transportation Information Sharing & Analysis Center |
| TCRP | Transit Cooperative Research Program |
| TEW | Terrorism Early Warning (Group) |
| TIFs | Threat Information Forums |
| TII | Transportation Information Infrastructure |
| TIOC | Transportation Information Operations Center |
| TSA | Transportation Security Administration |
| TTPs | Tactics, Techniques, & Procedures |
| TUGs | Threat User Groups |
| USDOT | United States Department of Transportation |

**This page has been intentionally left blank.**

## APPENDIX B: PUBLIC TRANSPORTATION SYSTEMS PERSONNEL SENT SURVEY RESEARCH INSTRUMENTS

| | |
|---|---|
| Armstrong, Ken B.<br>Safety & Security<br>Detroit People Mover<br>1420 Washington Blvd<br>Detroit, MI 48228<br>Phone: 313-224-2160<br>Fax: 313-224-2134<br>Email: Unknown | Bacchus, Garvin<br>Security<br>Jacksonville Transportation Authority<br>100 N Myrtle Ave<br>Jacksonville, FL 32203<br>Phone: 904-630-3123<br>Fax: 904-630-3168<br>Email: garvinb@itaonthemove.com |
| Byrd, Robert<br>Chief of Police<br>Northern Indiana Commuter<br>Transportation District (NICTD)<br>33 East US Highway 12<br>Chesterton, IN 46304<br>Phone: 219-926-5744<br>Fax: 219-926-4438<br>Email: robert.byrd@nictd.com | Cook, Wayne<br>Director of Transportation<br>Galveston Island Transit<br>3115 Market Street<br>Galveston, TX 77550<br>Phone: 409-797-3900<br>Fax: 409-797-3901<br>Email: cookway@cityofgalveston.org |
| Cox, Charles<br>King County Metro<br>King County Courthouse<br>516 Third Avenue<br>Seattle, WA 98104<br>Phone: 206-684-2764<br>Fax: Unknown<br>Email: chuck.cox@metrokc.gov | Dart, Robert<br>Chicago Transit Authority<br>CTA Main Offices, PO Box 3555<br>Merchandise Mart Plaza, 7th Floor,<br>Chicago, IL 60654<br>Phone: 312-664-2997<br>Fax: Unknown<br>Email: CmdrDart@TransitChicago.com |
| Diaz, Joe<br>Safety & Security Manager<br>Hillsborough Area Regional Transit<br>4305 E 21st Avenue<br>Tampa, FL 33605<br>Phone: 813-623-5835<br>Fax: 813-623-5836<br>Email: diazj@hartline.org | Evans, Richard<br>SEPTA Police Department<br>Southeastern Pennsylvania<br>Transportation Authority (SEPTA)<br>1234 Market Street<br>Philadelphia, PA 19107-3780<br>Phone: 215-580-3640<br>Fax: Unknown<br>Email: chiefevans@hotmail.com |
| Findling, Larry<br>Tri-Met (Oregon)<br>Tri-County Metropolitan Transportation<br>District of Oregon (Tri-Met)<br>4012 SE 17th Avenue<br>Portland, OR 97202<br>Phone: 503-238-5835<br>Fax: Unknown<br>Email: findlinl@trimet.org | Fleming, William<br>Deputy Chief<br>Massachusetts Bay Transportation<br>Authority (MBTA)<br>240 Southampton Street<br>Boston, MA 02118-2723<br>Phone: 617-222-1121<br>Fax: 617-222-1035<br>Email: wfleming@mbta.com |

| | |
|---|---|
| Foster, Bernard<br>MTA of Maryland<br>Maryland Transportation Authority<br>303 Authority Drive<br>Baltimore MD 21222<br>Phone: 410-333-8141<br>Fax: Unknown<br>Email: Unknown | Frank, Raymond<br>Chief of Security<br>Santa Clara Valley Transportation Authority<br>3331 N 1st Street Building B-2<br>San Jose, CA 95134-1906<br>Phone: 408-321-7175<br>Fax: 408-955-0953<br>Email: ray_frank@vta.org |
| Gee, Gary<br>Chief of Police<br>Bay Area Rapid Transit (BART)<br>800 Madison Street<br>Oakland, CA 94607<br>Phone: 510-464-7022<br>Fax: 510-464-7024<br>Email: ggee@bart.gov | Genova, David<br>Manager of Public Safety<br>Regional Transit District<br>1900 31st Street<br>Denver, CO 80216<br>Phone: 303-299-4038<br>Fax: 303-299-3110<br>Email: david.genova@rtd-denver.com |
| Gillerson, Murray<br>Director of Operations<br>Central Arkansas Transit Authority<br>901 Maple Street<br>North Little Rock, AR 72114<br>Phone: 501-370-5813<br>Fax: 501-375-6812<br>Email: mgillerson@cat.org | Grote, Wulf<br>Sr. Transit Facility Engineer<br>Regional Public Transportation Authority<br>302 N. 1st Ave. Suite 700<br>Phoenix, AZ 85003<br>Phone: 602-262-7242<br>Fax: 602-534-0879<br>Email: wgrote@vm.maricopa.gov |
| Hill, James E.<br>Chief of Police<br>Administration Offices & Maintenance Facility<br>Port Authority Transit Corporation<br>Camden, NJ 08103<br>Phone: 856-963-7988<br>Fax: 856-963-7999<br>Email: jhill@drpa.org | Howard, Lt. Melvin<br>Security<br>Regional Transit Authority<br>2817 Canal St<br>New Orleans, LA 70119<br>Phone: 504-827-7910<br>Fax: 504-827-7928<br>Email: mhoward@norta.com |
| Joyce, John K.<br>Chief of Police<br>Greater Cleveland Regional Transit Authority<br>1240 West Sixth Street<br>Cleveland, OH 44113<br>Phone: 216-566-5174<br>Fax: 216-771-4809<br>Email: jjoyce@gcrta.org | Killbrew, Judd<br>Safety & Security<br>Memphis Area Transit Authority<br>1370 Levee Road<br>Memphis, TN 38108<br>Phone: 901-722-0303<br>Fax: 901-722-7142<br>Email: jkillbrew@matatransit.com |

| | |
|---|---|
| Lambert, Tom<br>Metro Transit of Harris County<br>1201 Louisiana<br>P.O. Box 61429<br>Houston, TX 77208-1429<br>Phone: 713-615-6409<br>Fax: Unknown<br>Email: t10@hou-metro.harris.tx.us | Lamph, David<br>Public Safety/Security Administrator<br>Utah Transit Authority<br>613 West 6960 South<br>Midvale, UT 84047<br>Phone: 801-352-6644<br>Fax: 801-352-6641<br>Email: dlamph@uta.cog.ut.us |
| Lawlor, Jim<br>General Manager<br>Kenosha Transit Commission<br>3735 65th Street<br>Kenosha, WI 53142<br>Phone: 262-653-4290<br>Fax: 262-653-4295<br>Email: coken2@execpc.com | Lennon, Paul<br>Los Angeles County Metropolitan<br>Transportation Authority (LA MTA)<br>One Gateway Plaza<br>Los Angeles, CA 90012-2952<br>Phone: 213-922-4418<br>Fax: Unknown<br>Email: lennon@mta.net |
| Lonergan, Mark<br>Deputy Chief Operating Officer<br>Sacramento Regional Transit District<br>PO Box 2110<br>Sacramento, CA 95812-2110<br>Phone: 916-321-2980<br>Fax: Unknown<br>Email: cbeach@sacrt.com | McCauley, Sgt. Steve<br>Security<br>Port Authority of Allegheny County<br>Heinz 57 Center 345 6th Ave<br>Pittsburgh, PA 15222-2527<br>Phone: 412-255-1500<br>Fax: 412-255-1352<br>Email: smccauley@portauthority.org |
| McDevitt, Barry<br>WMATA PD<br>Washington Metropolitan Area Transit Authority<br>600 Fifth Street, NW<br>Washington, DC 20001<br>Phone: 202-962-2150<br>Fax: Unknown<br>Email: bMcdevitt@wmata.com | McKinney, Joe<br>Deputy Chief<br>Metropolitan Atlanta Rapid Transit Authority (MARTA)<br>2424 Piedmont Road SE<br>Atlanta, GA 30324-3330<br>Phone: 404-848-4900<br>Fax: 404-848-5005<br>Email: jmckinney@itsmarta.com |
| Moore, Rick<br>Security & Fare Enforcement<br>Bi-State Development Agency<br>707 North First Street<br>St Louis, MO 63102-2595<br>Phone: 314-982-1507<br>Fax: 314-923-3032<br>Email: rmoore@bsda-transit.org | Nellegar, John<br>Acting Assistant General Manager,<br>Bus & Light Rail Safety<br>New Jersey Transit, Newark City Subway<br>180 Boyden Ave<br>Maplewood, NJ 07040-8484<br>Phone: 973-378-6061<br>Fax: 973-378-6824<br>Email: jnellegar@njtransit.com |

| | |
|---|---|
| Nelson, Jack<br>Transit Security Director<br>Metropolitan Council, Metropolitan Transit<br>2425 Minnehaha Avenue South<br>Minneapolis, MN 55404<br>Phone: 612-349-7237<br>Fax: 952-349-7299<br>Email: jack.nelson@metc.state.mn.us | O'Connor, John<br>Chief of Police and Special Units<br>Amtrak – Penn Station<br>31st and 7th Ave<br>NY, NY 10001<br>Phone: 212-630-7107<br>Fax: Unknown<br>Email: oconojh@amtrak.com |
| O'Donnell, James<br>MTA Police (NY)<br>347 Madison Avenue<br>New York, NY 10017<br>Phone: 212-878-1146<br>Fax: Unknown<br>Email: jodonnel@mtahq.org | Parks, James E.<br>Director of Operations<br>Cambria County Transit Authority<br>726 Central Avenue<br>Johnstown, PA 15902<br>Phone: 814-535-5526, Ext: 214<br>Fax: 814-536-5951<br>Email: jparks726@hotmail.com |
| Portuguez, Dan<br>San Diego Trolley<br>12555 Imperial Avenue, Suite 900<br>San Diego, CA 920101<br>Phone: 619-595-4940<br>Fax: 619-231-6760<br>Email: dportuguez@sdti.sdmts.com<br>Website: www.sandag.cog.ca.us/sdmts/ | Riga, Joseph<br>Chief of Transit Police<br>Niagara Frontier Transportation Authority<br>1404 Main Street<br>Buffalo, NY 14209<br>Phone: 716-855-7666<br>Fax: 716-855-7662<br>Email: Unknown |
| Roberson, John W.<br>Chief Engineer<br>Triangle Transit Authority<br>PO Box 13787<br>RTP, NC 27709<br>Phone: 919-485-7421<br>Fax: 919-485-7441<br>Email: jroberson@ridetta.org | Rodriguez, Juan M.<br>Chief of Transit Police<br>Dallas Area Rapid Transit<br>1401 Pacific Avenue PO Box 660163<br>Dallas, TX 75266-7288<br>Phone: 214-928-6320<br>Fax: 214-928-6357<br>Email: jrodrigu@dart.org |
| Todd, Bonnie<br>Chief, Transit Safety & Security<br>Metro-Dade Transit Agency<br>111 N.W. 1st Street 9th Floor<br>Miami, FL 33128<br>Phone: 305-375-4240<br>Fax: 305-375-3380<br>Email: btodd@co.miami-dade.fl.us | |

## APPENDIX C: SURVEY INSTRUMENT AND TRANSMITTAL LETTER

### SURVEY INSTRUMENT

### BACKGROUND AND CONTACT INFORMATION

This survey is being conducted to support a research task order from the Transit Cooperative Research Program (TCRP), a unit of the Transportation Research Board (TRB) of the National Academy of Sciences, and fits within a larger effort to conduct research in responding to the transportation sector's homeland security needs. Survey results will be reviewed to determine the viability of developing surface transportation threat protocols and corresponding threat dissemination systems. The research team for this effort is comprised of John Sullivan, Matthew Devost and James Kirkhope.

Please submit completed surveys to:

Transportation Communication Survey c/o Terrorism Research Center, Inc. (TRC)
5765-F Burke Centre Parkway, PMB 331
Burke, VA 22015
email: kirkhope@terrorism.com
fax: 703-935-2666

### Purpose of the Survey

The purpose of this survey is to evaluate the requirements of the transit environment to develop a series of protocols for event reporting and profiles for how information should be distributed. Several transit operators are currently participating in this effort with a goal to derive a series of working protocols and information flow diagrams detailing when and how threat information should be disseminated and how to recognize trends that might be indicative of a coordinated attack against multiple transit systems. (This process used for protocol development mirrors an earlier effort utilized by law enforcement agencies to develop protocols for response and dissemination of terrorism threat data). Our goal is to determine the current information sharing mechanisms and threat information needs of transit operators and security (including police) providers. The survey will also attempt to determine preferences for system design, interoperability, and information surety (operational security).

### Survey Instructions

Please fill out this brief survey as completely as possible and return by **Tuesday, May 7, 2002.**

**Section 1 - Background Information**

| Contact Person/Survey Respondent: | |
|---|---|
| Transit Operator: | |
| Address: | |
| Phone: | Fax: |
| Email: | Web Address: |

Transportation System Includes (check all that apply):

| Airport | Bus | Ferry | Highway/bridge |
|---|---|---|---|
| Light Rail/Subway/etc. | Paratransit | Port | Rail |
| Other – please describe: | | | |

Does Transport System have its own police department? (Circle one) Yes No

Does Transport System have its own security department? (Circle one) Yes No

Estimated Number of Threat Warnings:

| 1998: | 1999: | 2000: | 2001: |
|---|---|---|---|

Estimated Number of Actual Threat Incidents (to which personnel were dispatched):

| 1998: | 1999: | 2000: | 2001: |
|---|---|---|---|

**Section 2 – Assessment of Current Practices**

Current Sources of Threat Communications (check as many as apply)
Please rate the importance of each type of transmission to your operation.
(Scale of 1-7 with 1 least important and 7 most important):

| BOLO (be on the look out)/Wanted persons | National Crime Information Center |
|---|---|
| Broadcast of attacks (open source) | News reportage (open source intelligence) |
| Current threats (advisories, alerts and warnings) | NIPC |
| FBI InfraGard | Office of Intelligence and Security |
| FRA | State law enforcement |
| FTA | Training opportunities (i.e., WMD or |

| | |
|---|---|
| | counter-terrorism training |
| Homeland Security Advisory System (HSAS) Threat level | TTPs - Advisories on terrorist tactics, techniques and procedures |
| Internet (listserves, bulletin board, etc.) | USDOT |
| Lessons learned | Other (specify) |
| Local emergency management | |
| Local law enforcement | |

Have you been briefed on the Homeland Security Advisory System (HSAS)? (Circle one) Yes No

Have you integrated the HSAS into your existing threat communication protocol? (Circle one below)
Yes – if so, how?
No

Methods (rate timeliness: Scale 1 – 7 and Utility: Scale 1 – 7) 1=slow/not useful 7=fast/extremely useful

| *Threat Communication Medium* | *Timeliness* | *Utility* |
|---|---|---|
| Cell Phone | | |
| Email | | |
| Fax | | |
| Line Phone | | |
| Pager/Blackberry | | |
| Surface Mail/Postal Service | | |

Do you utilize current threat advisories to modify operational status of the system or enhance/modify security posture? (Circle one below)
Yes – if so, how?
No

Do you coordinate your security posture with proximate or connecting transit systems? (Circle one below)
Yes – if so, how?
No

Who/What position is responsible for determining threat and level in your system?

| |
|---|

**Section 3 – Assessment of Operational Needs (Preferences)**

For any proposed transportation threat communication system, please rate the importance of the following:
(Scale of 1-7 with 1 least important and 7 most important):

| | |
|---|---|
| message vetting and authentication | historical evaluation (i.e., for trend analysis) |
| message archiving, | peer-to-peer communication. |

To what media should a new integrated transportation threat communication system link? (check all that apply):

| | | |
|---|---|---|
| Cellular systems | Internet | Pagers |
| Other (please specify): | | |

Would a web-based system for threat communication meet your needs? (Circle one)
Yes No

If Yes,

| | | |
|---|---|---|
| Should there be a public and restricted access side | Yes | No |
| Should there be tiers of access (levels of access for types of personnel, e.g. one level for transit operations, a higher level for police, etc.)<br>If Yes, please provide suggestions: | Yes | No |
| Please suggest what kind of password/user identification is desirable: | | |

Please provide suggestions on the following topics for design of a new integrated transportation threat communication system:

System design

Interoperability

Information surety (operational security)

What level of security

Current information sharing mechanisms

Threat information needs

**Comments/Suggestions for Improved Communication of Threats:**

**Questions to Survey Administrators:**

Date survey completed:_____
For clarifications please contact **James Kirkhope:**
(Tel: 703-380-9194), (Fax:703-935-2666), kirkhopes@terrorism.com

**TRANSMITTAL LETTER**

Dear Sir:

We are conducting a survey to evaluate the requirements of the transit environment to develop a series of protocols for event reporting and profiles for how information should be distributed.

This survey is supporting a research task order from the Transit Cooperative Research Program (TCRP), a unit of the Transportation Research Board (TRB) of the National Academy of Sciences. Additionally, it fits within a larger effort to conduct research in responding to the transportation sector's homeland security needs.

Several transit operators are currently participating in this effort with a goal to derive a series of working protocols and information flow diagrams detailing when and how threat information should be disseminated and how to recognize trends that might be indicative of a coordinated attack against multiple transit systems. (This process used for protocol development mirrors an earlier effort utilized by law enforcement agencies to develop protocols for response and dissemination of terrorism threat data).

Our goal is to determine the current information sharing mechanisms and threat information needs of transit operators and security (including police) providers. The survey will also attempt to determine preferences for system design, interoperability, and information surety (operational security).

Survey results will be reviewed to determine the viability of developing surface transportation threat protocols and corresponding threat dissemination systems. The research team for this effort is comprised of John Sullivan, Matthew Devost and James Kirkhope (survey point of contact).

Please feel free to contact us with any questions or comments. I will follow up shortly with a phone call to confirm receipt of the attached survey.

Sincerely,

James Kirkhope
Transportation Communication Survey Coordinator
Terrorism Research Center

Tel: 730-380-9194
Fax: 703-935-2666
email: kirkhope@terrorism.com

## APPENDIX D: HOMELAND SECURITY ADVISORY SYSTEM (HSAS) CONDITIONS

### LOW CONDITION/GREEN

*Low risk of terrorist attacks.* The following protective measures may be applied:

- ❒ refining and exercising preplanned protective measures;
- ❒ ensuring personnel receive training on HSAS, departmental, or agency-specific protective measures; and
- ❒ regularly assessing facilities for vulnerabilities and taking measures to reduce them.

### GUARDED CONDITION/BLUE

*General risk of terrorist attack.* In addition to the previously outlined protective measures, the following may be applied:

- ❒ checking communications with designated emergency response or command locations;
- ❒ reviewing and updating emergency response procedures; and
- ❒ providing the public with necessary information.

### ELEVATED CONDITION/YELLOW

*Significant risk of terrorist attacks.* In addition to the previously outlined protective measures, the following may be applied:

- ❒ increasing surveillance of critical locations;
- ❒ coordinating emergency plans with nearby jurisdictions;
- ❒ assessing further refinement of protective measures within the context of the current threat information; and
- ❒ implementing, as appropriate, contingency and emergency response plans.

### HIGH CONDITION/ORANGE

*High risk of terrorist attacks.* In addition to the previously outlined protective measures, the following may be applied:

- ❒ coordinating necessary security efforts with armed forces or law enforcement agencies;
- ❒ taking additional precaution at public events;
- ❒ preparing to work at an alternate site or with a dispersed workforce; and
- ❒ restricting access to essential personnel only.

## SEVERE CONDITION/RED

*Severe risk of terrorist attacks.* In addition to the previously outlined protective measures, the following may be applied:

- ❒ assigning emergency response personnel and pre-positioning specially trained teams;
- ❒ monitoring, redirecting or constraining transportation systems;
- ❒ closing public and government facilities; and
- ❒ increasing or redirecting personnel to address critical emergency needs.

## APPENDIX E: PROPOSED NEXT STEPS

The following discussion delineates an initial suggested course of action to develop the framework system discussed in the body of this report.

### TASK 1: DEVELOP FUNCTIONAL REQUIREMENTS DOCUMENTATION

A functional requirements document should be developed defining the following elements:

- the end-state TIF portal (including plans for security, information exchange, and information management);
- an estimated cost-plan for achieving full functionality using an incremental and scalable development approach;
- a beta-test plan for ensuring that the public transportation system's stakeholders can provide constant feedback to ensure the portal functionality meets their requirements; and
- an integration plan for interfacing with other local and national level information sharing initiatives (e.g., InfraGard and/or TEW) and examining potential placement of the TIF within an existing entity, such as the ST-ISAC. This effort should include liaison and outreach to these entities.

An initial ballpark estimate for accomplishing this task ranges from $100,000 to $125,000.[9] It is anticipated that the period of performance to accomplish this task would be approximately four to six months.

### TASK 2: BETA SYSTEM DEVELOPMENT

It is suggested that a beta system with limited functionality be developed and tested with select representatives of the public transportation community. The beta system should be capable of collecting, storing, and disseminating threat information via secure Web and email. Extensive beta testing should be conducted with feedback incorporated into the final portal implementation.

An initial ballpark estimate for accomplishing this task ranges from $600,000 to $800,000.[10] A more specific cost estimate would be refined based on the establishment

[9] Note that this is an initial estimated cost that would need further refinement.

[10] An estimated cost for Tasks 2 & 3 is provided based upon the experience of the members of the MTA research team who have been involved in the development of the functional requirements for other systems and in the design of similar systems. A more detailed cost estimate would be generated during Task 1 of an expanded project. This cost estimate could be used as the basis for a development contract to initially establish the prototype system.

of the specific requirements. It is anticipated that the period of performance to accomplish this task would be approximately 8 to 16 months.

## TASK 3: TIF PORTAL VERSION 1.0

It is suggested that the TIF Portal Version 1.0 be capable of collecting, storing and disseminating information via the mechanisms articulated in this report. Full documentation regarding the maintenance and management (including staffing requirements) of the TIF Portal should be developed along with recommendations for implementation in live mode at the regional or national level with a transitional plan for housing the system within the appropriate entity or implementing it as a stand alone capability.

An initial ballpark cost estimate for accomplishing this task ranges from $500,000 to $750,000, depending on where it would be housed and other questions that would need to be answered. As with the previous tasks, a more specific cost estimate would be refined based on the establishment of the specific requirements. The period of performance may range from 6 to 12 months.

The cost of developing the system as initially estimated in ballpark numbers is $1.2 million to $1.7 million, or less than 10% of the capitalization cost to implement the system. If these cost estimates were validated, the development cost of the system would indeed be a bargain.

## APPENDIX F: SURVEY RESULTS

### SECTION 1 - BACKGROUND INFORMATION

Transportation System Includes (check all that apply):

| | | | |
|---|---|---|---|
| Airport<br>**1** | Bus<br>**10** | Ferry<br>**0** | Highway/bridge<br>**1** |
| Light Rail/Subway/etc.<br>**8** | Paratransit<br>**9** | Port<br>**0** | Rail<br>**6** |
| Other – please describe:<br>"Commuter Rail" – 1 | | | |

Does Transport System have its own police department? **6** Yes, **6** No

Does Transport System have its own security department? **7** Yes, **4** No

Estimated Number of Threat Warnings:

| | | | |
|---|---|---|---|
| 1998:<br>**4** | 1999:<br>**6** | 2000:<br>**5** | 2001:<br>**24** |

Estimated Number of Actual Threat Incidents (to which personnel were dispatched):

| | | | |
|---|---|---|---|
| 1998:<br>**12** | 1999:<br>**12** | 2000:<br>**14** | 2001:<br>**25** |

### SECTION 2 – ASSESSMENT OF CURRENT PRACTICES

Current Sources of Threat Communications (check as many as apply)
Please rate the importance of each type of transmission to your operation.
(Scale of 1-7 with 1 least important and 7 most important):

| | |
|---|---|
| BOLO (be on the look out)/Wanted persons<br>**Average Score: 4.71**<br>Respondents: 7<br>Median: 4.5<br>Mode: 5, 7 | National Crime Information Center<br>**Average Score: 3.78**<br>Respondents: 9<br>Median: 4<br>Mode: 2,4 |
| Broadcast of attacks (open source)<br>**Average Score: 6.22**<br>Respondents: 9<br>Median: 6<br>Mode: 6 | News reportage (open source intelligence)<br>**Average Score: 4.78**<br>Respondents: 9<br>Median: 4<br>Mode: ? |
| Current threats (advisories, alerts, and warnings)<br>**Average Score: 4.82** | NIPC<br>**Average Score: 4.50**<br>Respondents: 4 |

| | |
|---|---|
| Respondents: 11<br>Median: 4.5<br>Mode: 6 | Median: 4<br>Mode: 7 |
| FBI InfraGard<br>**Average Score: 4.86**<br>Respondents: 7<br>Median: 4<br>Mode: 7 | Office of Intelligence and Security<br>**Average Score: 3.57**<br>Respondents: 7<br>Median: 4<br>Mode: 3 |
| FRA<br>**Average Score: 3.17**<br>Respondents: 6<br>Median: 4<br>Mode: 3 | State law enforcement<br>**Average Score: 4.73**<br>Respondents: 11<br>Median: 4<br>Mode: 7 |
| FTA<br>**Average Score: 5.80**<br>Respondents: 10<br>Median: 4<br>Mode: 7 | Training opportunities (i.e., WMD or counter-terrorism training)<br>**Average Score: 5.44**<br>Respondents: 9<br>Median: 5<br>Mode: 7 |
| Homeland Security Advisory System (HSAS) Threat level<br>**Average Score: 4.44**<br>Respondents: 9<br>Median: 4<br>Mode: 3,4,7 | TTPs – Advisories on terrorist tactics, techniques and procedures<br>**Average Score: 4.25**<br>Respondents: 8<br>Median: 4<br>Mode: 1,5,7 |
| Internet (listserves, bulletin board, etc.)<br>**Average Score: 4.11**<br>Respondents: 9<br>Median: 3.5<br>Mode: 6 | USDOT<br>**Average Score: 4.67**<br>Respondents: 9<br>Median: 4<br>Mode: 7 |
| Lessons learned<br>**Average Score: 5.14**<br>Respondents: 7<br>Median: 5<br>Mode: 5 | Other (specify)<br>CATIC – California Anti-Terrorism Information Center – 5<br>State OES – 6<br>FBI Joint Terrorism Task Force – 7 |
| Local emergency management<br>**Average Score: 5.50**<br>Respondents: 10<br>Median: 4<br>Mode: 7 | |
| Local law enforcement<br>**Average Score: 5.64**<br>Respondents: 11<br>Median: 4<br>Mode: 7 | |

Have you been briefed on the Homeland Security Advisory System (HSAS)?
**6** Yes, **5** No

Have you integrated the HSAS into your existing threat communication protocol?
**2** Yes, **9** No

If Yes, how?
"Formal protocol still in development within our committee that meets two times per month to address terrorism issues. Anticipate using threat level to determine adjustments in staffing, assignment of fixed posts at vulnerable points, etc."

Methods (rate timeliness: Scale 1 – 7 and Utility: Scale 1 – 7)
(1=slow/not useful 7=fast/extremely useful)

| *Threat Communication Medium* | *Timeliness* | *Utility* |
|---|---|---|
| Cell Phone<br>Respondents: 12 | **Average Score: 6.08**<br>Median: 4<br>Mode: 7 | **Average Score: 5.08**<br>Median: 4<br>Mode: 7 |
| Email<br>Respondents: 12 | **Average Score: 4.75**<br>Median: 4.5<br>Mode: 4 | **Average Score: 4.75**<br>Median: 4.5<br>Mode: 4 |
| Fax<br>Respondents: 12 | **Average Score: 4.58**<br>Median: 4<br>Mode: 4 | **Average Score: 4.67**<br>Median: 4<br>Mode: 4 |
| Line Phone<br>Respondents: 12 | **Average Score: 6.17**<br>Median: 5<br>Mode: 7 | **Average Score: 5.75**<br>Median: 5<br>Mode: 7 |
| Pager/Blackberry<br>Respondents: 12 | **Average Score: 4.42**<br>Median: 4<br>Mode: 6 | **Average Score: 3.83**<br>Median: 4<br>Mode: 1,2,4,5,6 |
| Surface Mail/Postal Service<br>Respondents: 11 | **Average Score: 1.45**<br>Median: 2<br>Mode: 7 | **Average Score: 1.91**<br>Median: 4<br>Mode: 1 |

Do you utilize current threat advisories to modify operational status of the system or enhance/modify security posture? **7** Yes, **5** No

If so, how?

- ❒ "Post additional security or law enforcement personnel or secure resources based on nature of threat."
- ❒ "Upgrade threat status based on assessments."
- ❒ "Possible redeployment and increase of security personnel. Heighten awareness of employees."
- ❒ "Use to determine need for extra shifts, staffing vulnerable points, etc."
- ❒ "Threat condition levels were established by General Order."

- ❒ "Heightened state of alerts."
- ❒ "Secure critical sites."

Do you coordinate your security posture with proximate or connecting transit systems? (Circle one below) **2** Yes, **10** No

If so, how?

- ❒ "If asked."
- ❒ "Communications with Metro Police."

Who/What position is responsible for determining threat and level in your system?

- ❒ "Chief, Office of Safety and Security"
- ❒ "Manager, System Security"
- ❒ "Security Manager"
- ❒ "President or Executive VP of Transit Operations"
- ❒ "Director"
- ❒ "Police Department Staff with advisory to District Staff"
- ❒ "Chief of Police"
- ❒ "Currently developing threat assessment committee"
- ❒ "Security Manager"
- ❒ "Chief of Police/Director of Security"
- ❒ "Chief of Police and General Manager"
- ❒ "Chief of Police (Transit)"

## SECTION 3 – ASSESSMENT OF OPERATIONAL NEEDS AND PREFERENCES

For any proposed transportation threat communication system, please rate the importance of the following:
(Scale of 1-7 with 1 least important and 7 most important):

| | |
|---|---|
| message vetting and authentication<br>Respondents: 11<br>**Average Score: 6.09**<br>Median: 4<br>Mode: 7 | historical evaluation (i.e., for trend analysis)<br>Respondents: 11<br>**Average Score: 4.64**<br>Median: 4.5<br>Mode: 5,6 |
| message archiving,<br>Respondents: 11<br>**Average Score: 3.73**<br>Median: 3.5<br>Mode: 4 | peer-to-peer communication<br>Respondents: 11<br>**Average Score: 6.00**<br>Median: 5.5<br>Mode: 7 |

To what media should a new integrated transportation threat communication system link?

| | | |
|---|---|---|
| Cellular systems **7** | Internet **9** | Pagers **7** |

| Other (please specify): |
|---|
| ❒ "Local police"<br>❒ "Fax and direct line communication to our 24 hour police dispatch center. Other contact points may be unavailable at a crucial time. Notification to the dispatch center will ensure correct personnel are available."<br>❒ "NCIC & state systems"<br>❒ "Land lines" |

Would a web-based system for threat communication meet your needs? **8** Yes, **3** No

If Yes,

| | | |
|---|---|---|
| Should there be a public and restricted access side | **8** Yes | **0** No |
| Should there be tiers of access (levels of access for types of personnel, e.g. one level for transit operations, a higher level for police, etc.)<br>If Yes, please provide suggestions:<br>❒ "Give local law enforcement all information."<br>❒ "Reserve criminal intel for law enforcement personnel only."<br>❒ "For Law enforcement only, for general distribution." | **8** Yes | **1** No |
| Please suggest what kind of password/user identification is desirable:<br>❒ "User specific alpha-numeric codes with periodic renewals."<br>❒ "That chosen by user."<br>❒ "Name and password."<br>❒ "Secure and Protected – monitored."<br>❒ "Encrypted." | | |

Please provide suggestions on the following topics for design of a new integrated transportation threat communication system:

**SYSTEM DESIGN**

- ❒ "Easy and fast to user."
- ❒ "Simple and redundant."
- ❒ "Constantly upgraded."
- ❒ "Our dispatch uses phone as communication tool. We will be part of combined communications system with public safety in the future. We are a small transit system and utilize our local police and fire departments as our security eyes and ears."

**INTEROPERABILITY**

- ❒ "Allow for ease of communication and/or integration with other agencies."
- ❒ "Make available all information sharing."
- ❒ "System should be 'user-friendly' to allow easy exchange of info with source and other similar agencies."

## INFORMATION SURETY (OPERATIONAL SECURITY)

- ❒ "Restrict access based on levels of responsibility."
- ❒ "Include all public safety entities."
- ❒ "Consider use of NCIC to distribute info to law enforcement agencies in a secure mode."

## WHAT LEVEL OF SECURITY

- ❒ "Allow select individuals at transit properties to have access similar to that maintained by law enforcement agencies."
- ❒ "All levels."
- ❒ "General Information (low)."
- ❒ "Specific Information (high)."
- ❒ "All levels."
- ❒ "Prefer the availability of 'law enforcement sensitive' information."
- ❒ "Top Secret Clearance."

## CURRENT INFORMATION SHARING MECHANISMS

- ❒ "Standardize bandwidth/radio frequencies/jargon, etc."
- ❒ "Email/web access."
- ❒ "The number of sources need to be consolidated."
- ❒ "Local law enforcement, FTA, FBI, Homeland Security National Alert System."
- ❒ "Through FBI JTTF, Bay Area Terrorism Working Group, state OES, local contacts."
- ❒ "Phone (cell), fax machine."

## THREAT INFORMATION NEEDS

- ❒ "Assessment of threats to identify credibility."
- ❒ "Pertains to our local area, then nationwide."
- ❒ "Timely."
- ❒ "RISS – would be advantage to public transportation systems."
- ❒ "Needs to be timely and some measure of how reliable the information is."

## COMMENTS/SUGGESTIONS FOR IMPROVED COMMUNICATION OF THREATS

"Most problems I have observed in transit agencies are from systems that do not have their own police department. We have had good cooperation from local FBI office and maintain liaison with several federal and state groups."

## QUESTIONS TO SURVEY ADMINISTRATORS

"How do you define 'threat warnings' and 'actual threat incidents?'"

The **Transportation Research Board** is a unit 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 draw on approximately 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.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. 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, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine 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 purpose 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 chairman and vice chairman, respectively, of the National Research Council.

Abbreviations used without definitions in TRB publications:

| | |
|---|---|
| AASHO | American Association of State Highway Officials |
| AASHTO | American Association of State Highway and Transportation Officials |
| ASCE | American Society of Civil Engineers |
| ASME | American Society of Mechanical Engineers |
| ASTM | American Society for Testing and Materials |
| FAA | Federal Aviation Administration |
| FHWA | Federal Highway Administration |
| FRA | Federal Railroad Administration |
| FTA | Federal Transit Administration |
| IEEE | Institute of Electrical and Electronics Engineers |
| ITE | Institute of Transportation Engineers |
| NCHRP | National Cooperative Highway Research Program |
| NCTRP | National Cooperative Transit Research and Development Program |
| NHTSA | National Highway Traffic Safety Administration |
| SAE | Society of Automotive Engineers |
| TCRP | Transit Cooperative Research Program |
| TRB | Transportation Research Board |
| U.S.DOT | United States Department of Transportation |

THE NATIONAL ACADEMIES

*Advisers to the Nation on Science, Engineering, and Medicine*

National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council

**TRANSPORTATION RESEARCH BOARD**
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

**ADDRESS SERVICE REQUESTED**

NON-PROFIT ORG.
U.S. POSTAGE
PAID
WASHINGTON, D.C.
PERMIT NO. 8970

83 P4
050657-00 TC086
RECEIVING
NATL TECH INFORMATION SERVICE
5285 PORT ROYAL RD
SPRINGFIELD VA 22161-0001