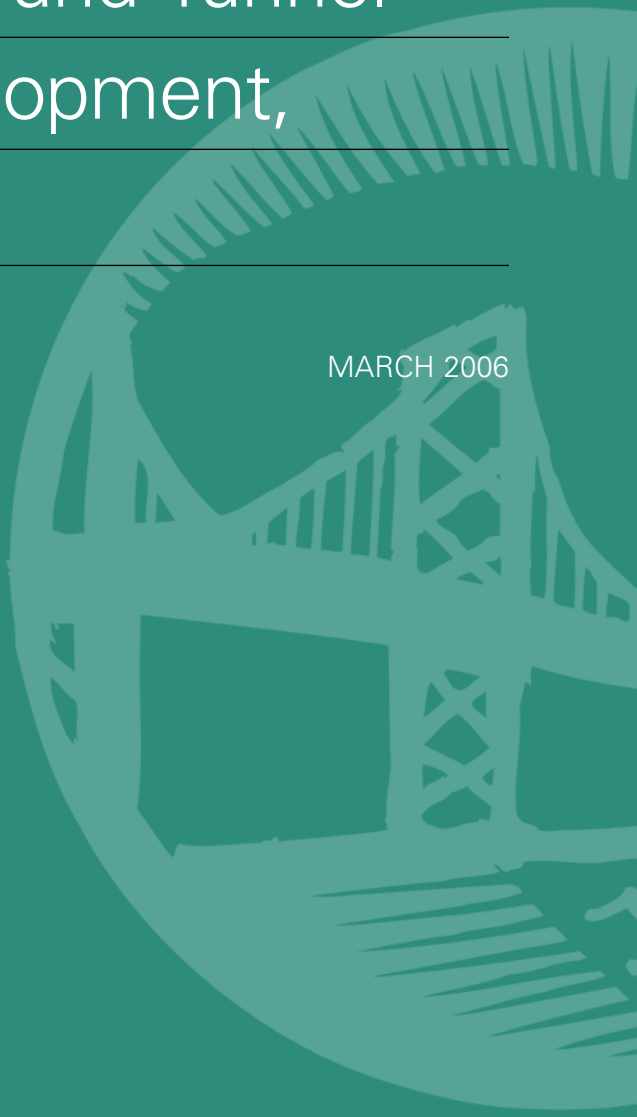
Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment

PUBLICATION NO. FHWA-HRT-06-072

MARCH 2006



U.S. Department of Transportation
Federal Highway Administration

Research, Development, and Technology
Turner-Fairbank Highway Research Center
6300 Georgetown Pike
McLean, VA 22101-2296

Foreword

Protecting critical infrastructure against terrorist events is a need imposed on us by the events of September 11, 2001. Although the transportation community has always responded to natural hazards, and there are procedures in place to design for and handle these, managing for terrorist events presents a new challenge. Transportation is essential for mobility and commerce, and it plays a critical role in times of crisis. Our highways are essential for evacuation, and in the response and recovery effort. However, our highways are also vulnerable, and can be used by terrorists as a means to carry out an attack. Because the challenge is tremendous, the Federal Highway Administration has been proactive by reaching out to stakeholders to identify critical gaps and needs. This has been accomplished through several forums as presented in this report. The input provided by experts in the field of bridge engineering and others has been evaluated and a program proposed to design highway bridges and tunnels for security.

Gary Henderson, Director
Office of Infrastructure
Research and Development

Notice

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-HRT-06-072		

4. Title and Subtitle	5. Report Date
Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment	March 2006
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Sheila Rimal Duwadi, P.E., and Steven B. Chase, Ph.D.	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Office of Infrastructure Research and Development Federal Highway Administration 6300 Georgetown Pike McLean, VA 22101-2296	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Office of Infrastructure Research and Development Federal Highway Administration 6300 Georgetown Pike McLean, VA 22101-2296	Final Report May 2002 – June 2005
	14. Sponsoring Agency Code HRDI-07

15. Supplementary Notes

16. Abstract

Transportation is identified as one of the critical infrastructures under Homeland Security Presidential Directive (HSPD) 7. It is essential for mobility and commerce, and plays a critical role in times of crisis. Our highways are essential for evacuation, and in the response and recovery effort. We have approximately 600,000 bridges and 300 tunnels on the highway network and many of these can be considered as being critical structures and/or on essential corridors. A damaged bridge or tunnel has an enormous impact on a city, a region, and possibly the Nation. Although the Federal Highway Administration (FHWA) has always been active in conducting research and development to mitigate natural hazards such as flooding and scour, earthquakes, wind, and wind-induced events, designing for security is a new task. Because the challenge is tremendous, FHWA has led multiple outreach sessions to identify needs and gaps. This input provided by experts in the field of bridge engineering and others has been evaluated and a program has been proposed to design highway bridges and tunnels for security.

17. Key Words	18. Distribution Statement
Security, bridges, tunnels.	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	59	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
		AREA		
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
		VOLUME		
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
	NOTE: volumes greater than 1000 L shall be shown in m^3			
		MASS		
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
		TEMPERATURE (exact degrees)		
^oF	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	^oC
		ILLUMINATION		
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	$candela/m^2$	cd/m^2
		FORCE and PRESSURE or STRESS		
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
		LENGTH		
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
		AREA		
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
		VOLUME		
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
		MASS		
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
		TEMPERATURE (exact degrees)		
^oC	Celsius	1.8C+32	Fahrenheit	^oF
		ILLUMINATION		
lx	lux	0.0929	foot-candles	fc
cd/m^2	$candela/m^2$	0.2919	foot-Lamberts	fl
		FORCE and PRESSURE or STRESS		
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380.
(Revised March 2003)

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

The Federal Highway Administration's (FHWA) national security strategic goal is to improve highway security and support national defense mobility through collaboration with the Department of Homeland Security (DHS) and our State, local government, private sector, and other Federal Agency partners. FHWA has further developed four objectives to meet this security strategic goal:

1. Develop a close working relationship with DHS and collaborate on establishment and implementation of highway-related security standards, administration of financial assistance for security initiatives, and distribution of threat and other sensitive security information to the highway industry.

2. Support national disaster preparedness, and response and recovery efforts.

3. Coordinate with our Nation's military and transportation owners/operators to ensure adequate transportation facilities and operation in support of military deployment.

4. Initiate and facilitate research and technology development in support of a more secure highway system

This report, developed by the Office of Infrastructure Research and Development (R&D), proposes a plan addressing objectives 2 and 4 above. The plan focuses on bridge and tunnel security. R&D associated with securing other parts of our national highway system is being addressed by other offices within FHWA.

It has been repeatedly stated that the surface transportation system is a resilient system, and except in a few major metropolitan areas and during peak periods, our national transportation network has significant redundancy (i.e., there are readily available alternate routes and alternate transportation modes). However, what is not so well documented is the enormous impact a damaged bridge or tunnel may have on a city, region, or possibly even the Nation's economy. This is especially true if the restoration and reopening of the damaged structure and/or network were to take an extended period of time, which will typically be the case for major structures. Because terrorism is an unpredictable event, it is more appropriate to rely on layers of security rather than on a single measure. In the long run, however, to ensure continued functionality of the Nation's physical infrastructure, it would be more appropriate to develop cost-effective designs utilizing improved materials, components, and structural systems, rather than relying solely on techniques for detection and surveillance.

SECTION 1: DEVELOPMENT OF A MULTIYEAR PROGRAM

This report proposes an R&D program addressing highway bridge and tunnel security. In addition to securing the physical infrastructure, it is recognized that there is a need to protect the "info infrastructure" as increasing reliance is placed on information technology as a result of the greater role being played by intelligent transportation systems. FHWA and other agencies within the U.S. Department of Transportation (DOT) must work together to address high-priority, long-term, long-range research needs in this and other areas in order to develop appropriate solutions at the national level.

Anticipating a multiyear program, FHWA initiated a number of efforts to identify research, development, and deployment needs for bridge and tunnel security. These efforts included a needs assessment, creation of a Blue Ribbon Panel, and conduct of a research needs workshop. The results of these activities are addressed below and form the multiyear bridge and tunnel security research program described herein.

During this same time period, the FHWA Office of Infrastructure R&D was restructuring its bridge and structures research program to pursue a more strategically focused R&D agenda. Realizing the worsening conditions of our bridges and other highway structures because of normal daily use, FHWA set a vision to "get out in front of the bridge deterioration curve and stay there," and to develop a strategy to conduct long-term, long-range research addressing: (1) design and construction needs to support development of the "Bridge of the Future"; (2) Stewardship and Management of our existing infrastructure; and (3) Safety, Reliability, and Security of both existing and future bridges and other highway structures. Therefore, when FHWA conducted a needs assessment, it included an outreach to both internal and external partners, customers, and stakeholders to help define gaps in knowledge and research needs within these three focus areas.

Requests were sent to both internal and external groups within the bridge community seeking input in structuring the bridge and structures R&D program. Subsequently, a series of meetings were held at FHWA's Turner-Fairbank Highway Research Center (TFHRC) where program managers and other invited FHWA offices assisted in refining the findings and restructuring the long-term R&D program. Results of this effort addressed needs in all three program focus areas. Presented herein are those needs addressing the security element of the bridge Safety, Reliability, and Security focus area. Although the discussion centers on bridge and tunnel security R&D, it should be realized that bridges and tunnels must be designed to withstand all hazards (natural and otherwise).

FHWA envisions a multiyear program that will lead to bridges and structures that are resilient to all extreme events and threats. In order to develop a resilient physical infrastructure that can withstand acts of terrorism, FHWA must invest in developing better risk and vulnerability assessment methodologies, newer structural systems and improved analysis techniques, and improved materials. The program should be structured to find improved ways to prevent incidents; however, if an incident does occur, it must also provide better methodologies for

assessing the safety of damaged structures. Investments must also be made to develop rapid repair and restoration techniques.

Overall, the program must encompass a wide range of topics that include systems analysis and design; improved materials; prevention, detection, and surveillance; post-event assessment, repair, and restoration; and evaluation and training.

SECTION 2: NEEDS ASSESSMENT, BLUE RIBBON PANEL, AND THE R&D SECURITY WORKSHOP

BACKGROUND

Needs Assessment

An initial outreach effort was conducted in August 2002. Research needs were generated by soliciting potential research projects from participants. This was accomplished through e-mails summarizing the purpose of the outreach effort and the information requested. The e-mails were directed in two groups, one to internal FHWA bridge engineers and a second to individuals and organizations outside of FHWA. More than 60 research needs for bridge and structures security were identified. Program managers were asked to solicit input from constituents. Organizations such as the Transportation Research Board (TRB), the American Association of State Highway and Transportation Officials (AASHTO), and the American Society of Civil Engineers (ASCE) circulated the request to their members.

Individuals in the following organizations and institutions were contacted as part of this outreach effort to determine research needs and gaps in knowledge in the security area:

- Society of Fire Protection Engineers
- Market Development Alliance
- American Society of Civil Engineers
- Building Futures Council
- American Portland Cement Alliance
- ITS America
- Transportation Research Board
- AASHTO
- U.S. Army Corps of Engineers, Engineer R&D Center, ERDC
- Pentagon Renovation Office
- Federal Facilities Council
- DOT, Research and Special Projects Administration
- National Institute of Standards and Technology
- Sandia National Laboratories
- Oak Ridge National Laboratory
- Caltrans
- Los Alamos National Laboratory
- Johns Hopkins University
- Multidisciplinary Center for Earthquake Engineering Research
- University of Texas
- University of Washington
- University of California at San Diego
- Iowa State University
- University of Michigan
- University of Delaware
- Drexel University
- CH2M Hill
- Intel Corporation
- Modjeski and Masters, Inc.
- Hardesty and Hanover, LLP
- T.Y. Lin International
- Wiss Janney Elstner Associates, Inc.
- HDR Engineering, Inc.
- FHWA, Office of Bridge Technology
- FHWA, Division Offices and Resource Centers

Blue Ribbon Panel

A Blue Ribbon Panel of bridge and tunnel experts representing professional practice, academia, and State and Federal agencies was convened to examine issues related to bridge and tunnel security, and to develop strategies and practices for deterring, disrupting, and mitigating potential attacks. Jointly sponsored by AASHTO and FHWA, and administered by TRB, the panel included:

James E. Roberts
Consulting Bridge Engineer
Imbsen and Associates, Inc.

Dwight Beranek
Deputy Director of Military Programs
U.S. Army Corps of Engineers

Joseph M. Englot
Chief Structural Engineer
Port Authority of NY and NJ

John W. Fisher, Ph.D.
Professor Emeritus
Lehigh University

Henry Hungerbeeler
Former Director
Missouri DOT

Jeremy Isenberg, Ph.D.
President and CEO
Weidlinger Associates, Inc.

John M. Kulicki, Ph.D.
President, CEO, and Chief Engineer
Modjeski and Masters, Inc.

Frieder Seible, Ph.D.
Dean, Jacobs School of Engineering
University of California, San Diego

Kenneth E. Stinson
Chairman and CEO
Peter Kiewit Sons', Inc.

Man Chung Tang, Ph.D.
Chairman of the Board and Technical Director
T.Y. Lin International

Kary Witt
Bridge Manager and Deputy General Manager
Golden Gate Bridge, Highway and Transportation District

In its report, *Recommendations for Bridge and Tunnel Security*, the Blue Ribbon Panel provides seven overarching recommendations in three areas—institutional, technical, and fiscal—required to accomplish the goal of reducing the vulnerability of bridges and tunnels to terrorist attacks. Recognizing that current design codes do not contain substantive information on how to employ hardening designs, quantify blast-related demands, and determine the capacity of components exposed to high-pressure transients, the report provides R&D recommendations for creating empirically validated computational tools, design methods, and hardening technologies.

R&D Security Workshop

FHWA held a workshop at TFHRC on March 3, 2004, to develop a strategic framework for R&D to improve security, focusing on highways and with an emphasis on longer range and more fundamental research needs. The product of this workshop was an unprioritized list of gaps and needs to help shape FHWA's strategic plan for R&D.

The workshop focused on three areas. The objective of each area was to identify gaps in current knowledge and technology that may prevent us from securing the Nation's highway

system. The first area focused on reducing the vulnerability of the Nation's highway system to attack, the second focused on reducing the risk of the highway system being used as a means to attack, and the third focused on improving the utility of the highway system to respond to and recover from an attack.

A total of 34 participants, representing a very broad cross section of disciplines, agencies, offices, and stakeholders, were invited to the workshop. Attendees included:

David Albright
New Mexico DOT

P.N. Balaguru
National Science Foundation

Rick Capka
Federal Highway Administration

Steven Chase
Federal Highway Administration

Ray Daddazio
Weidlinger Associates, Inc.

Fred Ducca
Federal Highway Administration

Sheila Rimal Duwadi
Federal Highway Administration

Steven L. Ernst
Federal Highway Administration

Brian Gardner
Federal Highway Administration

John Gerner
Federal Highway Administration

Monica Gourdine
Federal Highway Administration

Martin W. Hargrave
Federal Highway Administration

Amy Houser
Federal Motor Carrier Safety Administration, R&T

John Hoyt
Department of Homeland Security

Jeremy Isenberg
Weidlinger Associates, Inc.

Steve Jordan
Woodward Communications

Denny Judycki
Federal Highway Administration

Eva Lerner Lam
Palisades Consulting Group

Henry Lieu
Federal Highway Administration

Diane Liff
Federal Highway Administration

Michael P. Onder
Federal Highway Administration

Stephan Parker
Transportation Research Board

Vincent Pearce
Federal Highway Administration

Mary Lou Ralls
Texas DOT

James Ray
U.S. Army Corps of Engineers

Tamara Reid
AASHTO

John Rein
Department of Homeland Security

David Smith
Federal Highway Administration

Jim St. Pierre
National Institute of Standards and Technology

Paul Teng
Federal Highway Administration

Maliek van Laar
Woodward Communications

Anthony Welch
Federal Highway Administration

Jeff Western
Wisconsin DOT

RESULTS

These outreach efforts identified a variety of needs, research studies, and focus areas for securing our highways. As noted earlier, the needs assessment had an “all hazards” focus dealing with bridges and structures, while the work of the Blue Ribbon Panel concentrated on security issues and only those associated with bridges and tunnels, and the workshop concentrated on securing all highway transportation systems. Only those issues dealing with bridges and structures and with a security focus have been evaluated in developing the long-term program presented in this report. A summary of information resulting from the needs assessment, the Blue Ribbon Panel, and the workshop are given in appendixes A, B, and C, respectively.

SECTION 3: CURRENT PRACTICE AND GAPS IN KNOWLEDGE

The events of September 11, 2001, helped bring into focus the need to protect our highway system against terrorist incidents. Prior to September 11, these threats had always been perceived as minor, and, as such, little attention was paid to designing for security. Although the threat has been realized, there is still a struggle to define strategies and solutions to protect our highways against terrorism.

The larger civilian highway community has had little experience designing transportation infrastructure for security. Currently, our highway design codes and standards do not address loadings that might be experienced from terrorist activities, although research is slowly getting underway to change this. These issues, however, are not uncommon to the military. The military research community has long considered structural vulnerability of key structures in terms of how to attack those belonging to the enemy or how to make their own more resilient against enemy attack. The most complete experience with bridge vulnerability has come from numerous recent attacks of enemy bridges with large air-to-surface, precision-guided weapons. Much can be learned from these experiences; however, we can also reasonably assume that terrorist weapons would not be as sophisticated. Since the Oklahoma City bombing and attacks abroad on embassies, considerable work has also gone into the design of buildings for blast loadings. The U.S. Army Corps of Engineers (U.S. Army COE) has done considerable work in the area of conventional buildings and hardened structures subject to military weapons as well as terrorist attacks. The Department of State has supported considerable work in the area of blast/impact-resistant barrier designs. Technologies from these areas can be expanded to determine the applicability to highway structures.

In addition to bridges, the vulnerability of highway tunnels is an issue. The number of tunnels in the United States is growing because of a public preference for underground structures; the availability of better construction equipment and techniques; and the scarcity of above-ground space, especially in larger metropolitan areas. Highway tunnels are often considered to be relatively invulnerable to blast loadings, although there are major tunnels that may be highly susceptible to damage or collapse from a well-planned terrorist attack. A top priority in evaluating tunnel vulnerability to terrorist attacks is the threat of fire. Today, highway tunnels in the United States are designed in accordance with the National Fire Protection Association 502 Standard for Road Tunnels, Bridges, and Other Limited-Access Highways. Although tunnels are designed for fire, and there are restrictions on carrying explosives or other hazardous materials into tunnels, these restrictions are irrelevant when dealing with terrorist actions. Large amounts of explosives are not easily obtained, but it is a simple matter for terrorists to hijack trucks transporting gasoline or other flammable materials, and ignite them in the middle of a long tunnel. Recent accidents in the Mount Blanc and English Channel tunnels have shown that an intense fire and the resulting smoke can be a major threat in tunnels, can cause heavy casualties, and shut a tunnel down for months. Flammable materials, such as gasoline, propane, methane, propylene oxide, etc., can cause a blast problem similar to high-explosive detonation, in addition to fire.

Although there is a wealth of knowledge to be gained from the military, the national laboratories, and also from the mining industry, etc., this information is pretty much unknown to the owners of our highway infrastructure. The needs assessments highlighted current gaps in knowledge in the areas of structural vulnerability to terrorist events, threat definition, structural loadings produced by these threats, possible attack locations, cost-benefit and risk assessment methodologies, post-event assessment strategies, and the need for rapid repair and restoration techniques.

The ideas put forth during the workshop dealt with the overall transportation system. The need to develop a risk assessment methodology specific to highways was emphasized. Risk assessment methodologies are well developed and have been applied to many sectors for many years. However, there are many new and special aspects to the problem of applying existing methodologies to reduce the vulnerability of highways to attack. An essential input to a risk assessment is the event or scenario being analyzed. In the context of risk assessment of a terrorist or security event, the group felt that there was not adequate understanding of the "real" threats. Gathering and analysis of intelligence has not been a key competency or capability in the highway industry. This points to a need for better communication between those involved in the gathering of intelligence and those performing risk assessments. Validated models and tools, utilizing computer-based simulations, are needed to better analyze and quantify the consequences of and develop countermeasures to these threats. The need to develop improved surveillance and sensing technology to provide the data necessary to support the application of these advanced analysis and simulation tools was also identified as an area where research is needed.

In terms of reducing the risk of the highway system being used as a means to attack, the majority of the ideas from the workshop could be grouped into three areas: (1) surveillance technologies and decision support, (2) application of such systems to cargo or freight tracking with an emphasis on hazardous materials management, and (3) socio-political issues. Sensing, surveillance, and decision support includes the development and use of sensors and surveillance technologies to detect threats, the integration of such technologies into command and control systems, and the actual use of such systems to reduce the threat of the highway system to deliver an attack and, at the same time, the use of these systems to improve the operational efficiency of the highways to move freight and improve the safety of hazardous materials shipments. There was at least an implied perception that freight movement, cargo, and hazardous materials issues represent the most important way in which the highway systems can be used to deliver an attack. In addition, the linkage of the highway system with the transportation systems of foreign countries is predominantly associated with freight and cargo movement.

As for improving the utility of the highway system to respond to and recover from an incident, the workshop pointed out the need for better transportation management in a crisis situation, fundamental research in traffic flow in a crisis, and ability to communicate effectively during a crisis. Other issues identified dealt with decontamination of highway assets and vehicles after biological, chemical, or radiological exposure, and the need for rapid repair and restoration to have the ability to respond and recover from an incident.

SECTION 4: NATIONAL PLAN FOR R&D IN SUPPORT OF CRITICAL INFRASTRUCTURE PROTECTION

Released by DHS and the White House Office of Science and Technology Policy (OSTP) in April 2005, this plan is the first annual version of the R&D roadmap for critical infrastructure protection required by Homeland Security Presidential Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*.[(1)] The plan is national in scope, integrating cyber, physical, and human elements, and focuses on identification of capabilities, needs, and gaps based on known threats. The critical infrastructure per HSPD-7 includes the following sectors and key resources: Agriculture and Food; Water; Public Health and Healthcare; Emergency Services; the Defense Industrial Base; Information Technology; Telecommunications; Energy; Transportation Systems; Banking and Finance; Chemical Postal and Shipping; National Monuments and Icons; Dams; Government Facilities; Commercial Facilities; and Nuclear Reactors, Materials, and Waste.

The HSPD-7 directive also requires the development of a National Infrastructure Protection Plan (NIPP). The development of the R&D plan was tasked to the Infrastructure Subcommittee of the National Science and Technology Council (NSTC), and was developed in coordination with the Interim NIPP released in February 2005.

This first R&D plan focuses on two items: (1) the creation of a baseline, including the identification of major research and technology development efforts within Federal Agencies; and (2) the articulation of a vision that takes into account future needs and identifies research gaps based on known threats. Agency capabilities and near-term plans were mapped to R&D focus areas. FHWA and other agencies within DOT were involved in this process.

The National Critical Infrastructure Protection (NCIP) R&D Plan is structured around nine themes:

- Detection and sensor systems.
- Protection and prevention.
- Entry and access portals.
- Insider threats.
- Analysis and decision support systems.
- Response, recovery, and reconstitution.
- New and emerging threats and vulnerabilities.
- Advanced infrastructure architectures and systems design.
- Human and social issues.

The nine themes are to address three strategic goals:

- National common operating picture for critical infrastructure.
- Next-generation computing and communications network with security “designed in” and inherent in all elements rather than added after the fact.
- Resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems.

SECTION 5: PROPOSED FHWA MULTIYEAR PROGRAM

FHWA envisions a multiyear program that addresses securing the existing infrastructure and that will lead to the next generation of bridges and structures that are resilient to this new threat.

Terrorist threats to bridges can include:

- Fire (can lead to buckling of steel beams and spalling of concrete).
- Impact (can lead to damage of piers, causing collapse of the superstructure, and failure of hangers, again resulting in collapse of the superstructure).
- Mechanical cutting devices (can lead to cutting of hangers, resulting in collapse of the superstructure).
- Corrosive chemicals.
- Blast or explosion (can lead to severe damage of the structure).

Terrorist threats to tunnels can include:

- Fire.
- Impact.
- Chemical/biological attack.
- Blast/explosion.

While we need to design for all threats, bombs constitute 60 percent of terrorist attacks worldwide.

STRATEGIC FOCUS AREAS

The proposed FHWA program focuses on the following strategic areas to reduce the threat of damage to the infrastructure so that there is minimal loss of life, the infrastructure can stay open for movement of people and goods, and there will be little or no impact on the economy.

The recommended strategic focus areas for bridge and tunnel security R&D include:

- Risk and Vulnerability Assessment.
- System Analysis and Design.
- Improved Materials.
- Prevention, Detection, and Surveillance.
- Post-Event Assessment.
- Repair and Restoration.
- Evaluation and Training.

RESEARCH PROGRAM GOALS

The following identifies the major goals for each of the seven strategic focus areas given above.

Risk and Vulnerability Assessment

Goal: Develop better decision support tools, and more relevant and uniform methodologies for assessing the risk to and vulnerability of the highway infrastructure.

System Analysis and Design

Goal: Develop new analysis and design methodologies for highway bridges and tunnels to minimize physical damage.

Improved Materials

Goal: Explore and develop new materials, and improve on current materials for the next generation of bridges and tunnels.

Prevention, Detection, and Surveillance

Goal: Adapt existing technologies and develop new technologies for better detection and surveillance and prevention of terrorist incidents.

Post-Event Assessment

Goal: Develop guidelines for assessing the safety of structures after an event.

Repair and Restoration

Goal: Develop better repair and restoration techniques to restore a structure to its original capacity.

Evaluation and Training

Goal: Test and evaluate new technologies, and develop training aids to transfer new technologies.

TIE-IN TO THE NATIONAL CRITICAL INFRASTRUCTURE PROTECTION R&D PLAN

Table 1 shows the relationship between the NCIP R&D theme areas and FHWA strategic focus areas. One of the goals of both plans is to have "*resilient, self-diagnosing, and self-healing physical (and cyber) infrastructure systems.*"

Table 1: Relationship between NCIP R&D theme areas and FHWA strategic focus areas.

NCIP R&D Theme Areas	FHWA Plan: Strategic Focus Areas						
	Risk and vulnerability assessment	System analysis and design	Improved materials	Prevention, detection and surveillance	Post-event assessment	Rapid repair and restoration	Evaluation and training
Detection and sensor systems				X	X		X
Protection and prevention		X	X	X			X
Entry and access portals							
Insider threats							
Analysis and decision support systems	X	X					X
Response, recovery, and reconstitution					X	X	X
New and emerging threats and vulnerabilities	X						X
Advanced infrastructure architectures and systems design		X	X			X	X
Human and social issues							

RESEARCH AND DEVELOPMENT RECOMMENDATIONS

Based on analysis of the outreach efforts, the following R&D priorities were developed. This list should be revisited annually to ensure its continuing relevance and to update as necessary.

The studies that have been or are close to being initiated by FHWA and others are italicized in table 2 and in the study descriptions that follow.

Table 2: Research studies.

Strategic Focus Areas	FY03	FY04	FY05	FY06	FY07	FY08	FY09
Risk and Vulnerability Assessment							
Synthesis of existing risk and vulnerability assessment methodologies							
Determination of levels of risk and probability of occurrence for each event, and development of consistent risk assessment methodology							
Development of criticality models for bridges and tunnels for incorporation into risk assessment models							
Lessons learned – Bridge demolition							
Guide to risk management of multimodal transportation infrastructure (NCHRP)							
System Analysis and Design							
Standardized blast response curves for bridges (develop vulnerability curves to allow engineers to design appropriate standoff devices to mitigate these threats) (FHWA/U.S. Army COE)							

Table 2: Research studies, continued.

Strategic Focus Areas	FY03	FY04	FY05	FY06	FY07	FY08	FY09
ConWep modifications for bridges (FHWA/U.S. Army COE)							
Validation of numerical modeling and analysis of steel bridge towers subjected to blast loadings (FHWA/U.S. Army COE)							
Assessment of bridge designs for structural vulnerability against terrorist events							
Assessment of tunnel designs to resist blast and fire							
Optimized designs for hazard loadings							
Catalog of optimized design solutions for each event							
Advanced physical and numerical modeling and simulation capabilities for predicting and understanding behavior under extreme events							
Blast-resistant designs – Impact attenuators – Structural cladding							
Structural vulnerability guide							
Blast effects and retrofit techniques for tunnels							
Making transportation tunnels safe and secure (NCHRP)							
Better protection of piers against impact and/or blast loadings							
Blast testing of full-scale, precast, prestressed concrete girder bridges (WA State DOT)							
Blast-resistant highway bridges: Design and detailing guidelines (NCHRP)							
Improved Materials							
Response modification devices							
Material performance under extreme event loadings							
Resistant materials and coatings for improved performance							
Shape-memory alloys for bridge structural applications							
Nanoscale science and engineering							
MEMS sensors research							
Prevention, Detection, and Surveillance							
Synthesis of bridge and tunnel surveillance and security technologies (FHWA)							
Hazard mitigation measures							
Sensing and monitoring technologies for extreme events							
Post-Event Assessment							
Forensic analysis of damaged structures to understand residual capacity and develop protocols for rapid assessment							
Inspection techniques for rapid safety assessment of damaged structures							
Damage assessment guide for extreme events							

Table 2: Research studies, continued.

Strategic Focus Areas	FY03	FY04	FY05	FY06	FY07	FY08	FY09
Repair and Restoration							
Emergency repair procedures							
Accelerated repair and restoration techniques for reconstruction after an event							
Evaluation and Training							
Vulnerability Assessment Workshops (FHWA/U.S. Army COE)							
Institute a HITEC-type evaluation program for bridge and tunnel security technologies							
FHWA Engineering Assessment Team (FHWA)							

A short narrative is given below for most of these initiatives.

Risk and Vulnerability Assessment

Goal: Develop better decision support tools and more relevant methodologies for risk and vulnerability assessment.

Synthesis of existing risk and vulnerability assessment methodologies: This project would have a multi-hazard approach. There is a need to develop consistency in the levels of risks used in design to safeguard structures from both natural and terrorist attacks. Designers apply different return intervals for various aspects of design, which may or may not relate to a consistent risk analysis. For flooding, roadways are allowed to overtop at return intervals anywhere from 10 to 50 years, depending on the class of road. For seismic hazards, a 2500-year event is often selected for retrofit designs. For wind hazards, a 20-year occurrence event is selected for construction, a 100-year event is used for strength, a 1000-year event is used for flutter during construction, and a 10,000-year event is used for flutter of the completed bridge. Currently, there is no basis for designing for security in the design codes and standards. A synthesis is needed to clarify the state of the practice and to determine the feasibility of reaching a consistent set of guidelines for evaluating risks and cost benefits for all hazards. This study would conduct a literature search and synthesize all available risk and vulnerability assessment methodologies for extreme events, including floods, wind events, earthquakes, blasts, overloads, and accidents (collisions, fires, etc.), and develop and recommend a framework for a consistent methodology for all extreme events. The literature search would also look at probability methods, such as those used in industrial reliability. The resulting document and recommended framework will be used by FHWA for developing a single risk and vulnerability methodology for all extreme events encountered by the Nation's highway bridges and tunnels.

Determination of levels of risk and probability of occurrence for each event, and development of consistent risk assessment methodology: This project would conduct a broad investigation and identify acceptable risk levels in designing for each hazard type and the basis for their use. It would identify recurrence interval or probability of occurrence for each extreme event for each risk level. It would study the patterns of recurrence and how well each method has worked, as well as the economic costs incurred after using the method. The extent of loss of life would also be researched. The project would recommend if a single set of consistent levels of risk for all

hazards is feasible. This study would start with analyzing results from separate analyses of individual hazards, selecting the level most likely to be satisfactory, and then comparing the projected effects of the new design events to those in use to determine if safety and cost are increased or reduced. Finally, this study would develop a risk assessment methodology utilizing the framework developed in the previous study.

Development of criticality models for bridges and tunnels for incorporation into risk assessment models: This study will add to the developed risk assessment methodology by providing criticality models for different events for each risk category.

Lessons learned – Bridge demolition: This study would gather pertinent information from demolition companies on demolitions of structures in order to learn from their experiences. The goal would be to learn the difficulty and ease of the job; explosives needed (how much, what type, shape and location of placement; analytical approaches used; software type; time on target required, etc.).

Guide to risk management of multimodal transportation infrastructure (NCHRP): This National Cooperative Highway Research Program (NCHRP) study is developing a guide that will provide State DOTs and other transportation entities with a risk management methodology that can be used to conduct threat, vulnerability, and criticality assessments of their facilities and to determine cost-effective countermeasures to prevent, detect, and reduce threats to assets on a multimodal basis. The product of this project will be a recommended replacement to the *2002 AASHTO Guide to Highway Vulnerability Assessment for Critical Identification and Protection*.

System Analysis and Design

Goal: Develop new analysis and design methodologies for highway bridges and tunnels to minimize physical damage.

Assessment of bridge designs for structural vulnerability against terrorist events: The goal of this project would be to investigate and identify key components of each bridge design type for vulnerability to blast loadings, fire, and intentional impact. A summary of activities may involve collecting common bridge designs from State highway agencies, such as the designs of representative I-girder, box girder, suspension, cable-stayed, curved girder, and slab-type bridges; categorizing hazard loadings into different levels or classes; reviewing and assessing each bridge design type subjected to the different levels or classes of hazard loadings; identifying vulnerable details; and recommending design solutions and/or vulnerable elements requiring further study. This study would also look at where information exits, past performances of bridges during these events. This may include gaining access to infrastructure performance from the military from bombings in wars, military combat demolition, and military research. Although the types of ammunition used by the terrorists would most likely not be as sophisticated, much can be learned about the vulnerability of bridges from this available data. The expected products would be a document identifying vulnerable details and recommended solutions for each bridge design type and recommendations for future work. This study would be followed by subsequent studies to develop optimized designs and countermeasures for mitigating and hardening structures for extreme events.

Assessment of tunnel designs to resist blast and fire: This project would parallel the above project, but would concentrate on tunnels. The goal would be to investigate and identify key components of tunnel design for vulnerability to blast and fire. Activities may involve collecting tunnel design types, including soil conditions; categorizing hazard loadings into different levels or classes of loadings; review and analysis of each design type, subjecting each to the different levels or classes of hazard loadings; determining the weaknesses of each type; and recommending design solutions. This study would also look at, where information exits, past performances of tunnels during these events. This may include gaining access to the military on performance of tunnels from bombings in wars, military combat demolition, and military research. Although the types of ammunition used by the terrorists would most likely not be as sophisticated, much can be learned about the vulnerability of tunnels from this available data. The expected products would be a document identifying vulnerable details, recommended solutions for each tunnel design type, and recommendations for future work.

Making transportation tunnels safe and secure (NCHRP): The objective of this NCHRP research study is to develop safety and security guidelines for owners and operators of transportation tunnels to use to identify: (1) critical locations; (2) potential structural improvements; (3) operational countermeasures; and (4) deployable, integrated systems for command, control, communications, and information. The guidelines are to be applicable across the spectrum of both accidental and intentional threats.

Optimized designs for hazard loadings: This would involve multiple studies to develop design solutions for vulnerable designs, details, or weaknesses identified in the previous studies. It involves tailoring vulnerable details of structures for mitigating the consequences of a blast, utilizing improved fire-resistant materials and designs, and designing solutions for resisting vehicle and vessel collisions for vulnerable structures.

Catalog of optimized design solutions for each event: This project would compile into one document all optimized design solutions for each extreme event. It would be a "how to design for …" manual with illustrations and information on what and what not to do for the bridge designer.

Advanced physical and numerical modeling and simulation capabilities for predicting and understanding behavior under extreme events: This study would develop analytical capabilities to be used for predicting the behavior of structures under extreme events. The product would be of use to researchers, code developers, and bridge designers for making decisions in lieu of experimental tests.

Blast-resistant designs – Impact attenuators – Structural cladding: Following the Oklahoma City bombing, the General Services Administration (GSA) developed a series of bomb-blast requirements for buildings. For example, the Federal Aviation Administration's Eastern Regional Headquarters building in Queens, NY, utilizes precast panels that meet the GSA's requirements. Basically, it is a self-supporting building structure built within a self-supporting facade. The walls provide the blast-zone loading with the concrete and steel reinforcing stressed within the elastic range. These walls are the primary protective elements that provide resistance in case of an explosion and are considered "hardened elements." The cladding used outside these walls consists of precast concrete architectural panels with laid-up brick. The facade is only nominally

supported by the concrete frame. They designed a bunker-type structure, but clad it with precast concrete and brick in such a way that it absorbs the initial force of a blast. There is a 101.6-millimeter (4-inch) gap between the building's architectural features and structural elements. The goal of the precast concrete is not to be protective to an exterior explosion, but to "peel away" in case of a bomb blast, providing protection and absorbing force. It takes the first hit and absorbs some of the force, minimizing damage that could be caused by collapsing. The backup concrete wall then takes most of the force. The precast concrete serves as a "crumple zone" to protect the rest of the structure.

A study should be conducted to determine the feasibility of using this or similar design concepts for critical components of bridges and tunnels, such as piers, pylons, towers, tunnel walls, etc. Using this concept, one could make the cladding sacrificial and save the structure. If determined to be feasible, second and subsequent phases could be initiated to develop the concept further and to test on actual bridge and tunnel critical components.

Blast-resistant highway bridges: Design and detailing guidelines: This NCHRP study involves developing guidelines for selecting analysis techniques and developing design and detailing guidelines, evaluating approaches to enhancing the performance of bridges subjected to blast loads, and developing guide specifications and a procedure for assessing bridge damage caused by explosions.

Structural vulnerability guide: Currently, there are no guidelines, specifications, tools, or experience to determine the structural vulnerability of infrastructure (bridges and tunnels) to terrorism. The *AASHTO Guide to Highway Vulnerability Assessment* deals more with susceptibility to an attack based on location and the importance of the structure. The FHWA/U.S. Army COE's Bridge and Tunnel Vulnerability Workshop deals with structural vulnerability in an attack because of blast loadings, irrespective of the location. The material for the workshop is based on the U.S. Army COE's experience with infrastructure research to support the military's objectives. According to the U.S. Army COE, little or no research has been done in the specific area of terrorist threats against bridges and tunnels. Numerous Federal Agencies conduct R&D on security measures against hostile attacks. R&D in related areas, particularly protection against natural disasters and accidents, may also be effective in preventing the destruction of structures from hostile attacks. This project would explore these areas to determine applicability to highway structures and to develop a structural vulnerability guide.

Blast effects and retrofit techniques for tunnels: Research to determine blast effects and to develop retrofit techniques may be needed for some tunnel types, especially those on soft or poor soils, underwater, and cut and cover tunnels. There may also be a need to look at improving ventilation systems, designing systems for mass evacuations, etc. Based on what was presented at the U.S. Army COE's Bridge and Tunnel Vulnerability Workshop, numerous explosive tests have been conducted for the military on tunnel design systems anticipated by the military. Almost all of these, however, have been on one-way tunnels (i.e., there is only one entrance in and out of the tunnel). These tunnels are used to store ammunition and as shelters, not for moving people. Some of these tunnels also have berms in front of the entrances, which can mitigate the blast energy. As such, the current research data possibly would not be applicable to vehicular tunnels. If an explosive is detonated in a vehicular tunnel, the blast energy has clear exits in two directions; therefore, the reflection waves might even be less. This project would

determine the blast effects on vehicular tunnels and develop retrofit techniques through analysis and testing.

Standardized blast response curves for bridges: This study is developing simple design aids to help engineers design bridges for blast loadings. The study will produce a standardized set of blast response curves for a generic set of common bridge elements, including decks exposed to deck-top detonations, steel and prestressed girders exposed to deck-top detonations, rectangular and wall-type piers exposed to side-on detonations, and a single-cell tower of a cable-stayed bridge exposed to side-on deck-level detonations.

Bridge-specific blast loading program: This study is developing a user-friendly computer program for consistent definition of blast loadings on bridges. The U.S. Army COE's current computer program, ConWep (Conventional Weapons Effects), is widely used within the engineering community to predict blast loadings on structures from conventional weapons, including terrorist-type vehicular bombs. This program was originally developed as an expedient and user-friendly tool for engineers concerned mostly with building structures. The graphical user interface (GUI) of this program will be modified to better facilitate bridge-specific problems. It will develop a user-friendly and bridge-specific GUI for reliable definition of key parameters such as weapon size, weapon standoff, weapon orientation in relation to the structural element, the overall size of the structure, and the size of the responding element of interest.

Validation of numerical modeling and analysis of steel bridge towers subjected to blast loadings: Most major long-span bridges in the United States are vulnerable to terrorism. They are high-visibility structures, with a potential for extensive media exposure and public reaction if an incident were to occur. As a result of the long spans, complicated designs, site locations, etc., these bridges have very high replacement costs and multiyear replacement construction periods. The potential for impacting regional and national economies is also greater because of the increased time for reconstruction. Many of these bridges serve as transportation arteries critical for emergency evacuation and for carrying lifelines besides vehicular traffic. This study will develop several numerical models and analysis validated through the construction of physical models subjected to large explosive devices detonated to determine the actual behavior of such towers. This study will further develop and test several hardening concepts for cellular steel bridge towers so that the performance of these towers can be well understood in the event of such an attack occurring after the hardening has been implemented.

Blast testing of full-scale, precast, prestressed concrete girder bridges: This study will: (1) assess the damage done to precast, prestressed girder bridges from a blast generated below the girders, (2) compare this damage with a blast generated on top of the bridge deck, and (3) develop recommendations for possible mitigation measures that would harden this type of bridge blast damage. Precast, prestressed concrete girder bridges are the most prevalent bridge design in the country.

Material Performance

Goal: Explore and develop new materials, and improve on current materials for the next generation of bridges and tunnels.

Response modification devices: This projects aims to develop and refine response modification devices such as dampers, isolation bearings, yielding devices, and shape-memory alloys. This project would also look into developing cladding systems that take the initial impact and thereby lessen the load on the main members. The project would take a multi-hazard approach in developing devices for hazard mitigation.

Material performance under extreme event loadings: The behavior of construction materials in bridges subjected to fire is a critical issue that has not been addressed adequately in the past. The behavior of new high-performance materials is even less understood, and the enhanced material characteristics may be even less suited for high-intensity fires, such as a burning tanker truck carrying liquid petroleum. Although accidents involving trucks carrying hazardous materials are a common occurrence, the risk is amplified as a result of terrorism. As a first step toward developing fire-resistant construction materials and protective coatings, the performance of both normal-strength and high-performance steel and concrete during a fire needs to be assessed. This study should lead to a better understanding of the performance of materials during explosive loadings and fires. The study would include materials such as normal-strength and high-performance steel and concrete. It would determine how much blast material (energy) and heat are needed to damage a structure constructed of these materials so that the structure is no longer functional. This information could be used to determine design loads and also design mitigation measures. If the load required to damage a structure is unreasonable, this would also let you know that nothing needs to be done.

Resistant materials and coatings for improved performance: This study aims to develop materials and coating systems that can be applied to highway structures that can resist high-intensity fires and absorb blast loadings.

Shape-memory alloys for bridge structural applications: Shape-memory alloys are metallic composite materials capable of changing shape and returning to their original form after stresses have been removed. These materials have been in existence for more than 30 years. Structures made of these materials hold promise for possessing energy-absorbing capabilities, enabling them to sustain high-velocity impacts or explosions. The materials hold promise for resisting seismic, blast, and high-impact loadings. Although some research is being conducted, most is concentrated on the seismic issue. This study would assess these alloys for mitigating terrorist-type loadings.

Nanoscale science and engineering research: Nanoscale science and engineering represents an opportunity to engineer materials/devices with novel characteristics. At approximately 1 to 100 nanometers (a nanometer is equal to one-billionth of a meter), clusters of atoms and molecules exhibit properties very different from those found at larger scales. Nanoscience is the creation of new materials, devices, and systems at the molecular level. It can significantly improve mechanical, optical, chemical, and electrical properties. Through nanoscience, it is possible to create ductile ceramics. Nanoscience materials enable radical design changes. The National

Nanotechnology Initiative is a White House initiative involving 10 agencies. TFHRC, through its Advanced Research Program, has a number of research studies in this area. The possibility of protecting structures against terrorist threats through the use of nanotechnology by providing new designs, new materials, and blast-resistant structures is a new area that should be explored. This would be long-range, high-risk research with the potential for a high payoff.

Nanoscience research areas include:

- Materials that perform well under extreme conditions of temperature and pressure. These can be strong, tough, ductile, lightweight, and low-failure materials.
- Smart materials such as paints that change color with temperature.
- Radiation-tolerant materials.
- Self-healing materials: Research is ongoing at the National Aeronautics and Space Administration's Langley Research Center on self-healing materials development to develop materials that will mend themselves if subjected to high-velocity projectile penetration. This technology has the potential for structural applications in bridges. Nanoscale self-healing materials can be developed to be embedded in structural materials that become activated at the site of a fracture, etc., and self-heal the material.

Nanotechnology can be used to build stronger, lighter, and harder materials as has already been done in the aerospace industry.

MEMS sensors research: Research into micro-electro-mechanical systems (MEMS) would be another high-risk, high-payoff research. Its application in structures can include structural monitoring and structural control, nondestructive evaluation, and materials engineering and analysis. MEMS sensors can be used to measure physical properties (temperature, pressure, strain, magnetism, etc.) and inertial properties (vibration, tilt, acceleration, and velocity); for chemical and particle detection, and range and motion detection; and for imaging. Examples of these sensors include silicon accelerometer, silicon gyro, micro-hotplate chemical sensors, and ion-mobility spectrometer and pressure sensors.

MEM sensors can be used to design for security. They are already a key element in improving the performance of concrete. Cyberliths are complete monitoring and telemetry systems on a chip that can be embedded in artificial pebbles and thrown in with the aggregates during the mixing of concrete. More sophisticated cyberliths could be developed to measure stress distributions. MEM methods have been applied to manufacture thousands of miniature ultrasonic transducers on a single chip. It is more powerful than conventional transducers and enables inspection by noncontact, nondestructive technology. MEM actuators can be used at selected locations to control structural vibrations. Nanosensors embedded in cables, piers, pylons, and decks could sense imminent danger or collapse and alert engineers. Nanosensors embedded at various locations on a structure could act as the "brain" of the bridge and alert authorities to multiple hazards.

Prevention, Monitoring, Detection, and Surveillance

Goal: Adapt existing technologies and develop new technologies for better monitoring, detection, surveillance, and prevention of incidents, catastrophic failures, and/or condition assessment.

Synthesis of bridge surveillance and security techniques: This study is synthesizing the state-of-the-art practices related to surveillance and security of our bridge structures, and developing an evaluation framework to select among alternative surveillance and security approaches.

Hazard mitigation measures: This project would include studies to develop countermeasures for mitigating hazards. It would include blast mitigations systems and impact absorption devices.

Sensing and monitoring technologies for extreme events: This project would develop sensing and monitoring technologies that can be incorporated into our bridges and structures to monitor performance during extreme events, detect intruders, and help assess the post-event capacity of structures. It would include developing monitoring and warning devices to prevent vehicle collisions on bridge girders and vessel collisions at bridge piers. It would also include developing monitoring and warning devices to predict bridge scour, movement of bridge piers, and aerodynamic instability.

Post-Event Assessment

Goal: Develop guidelines and methodologies for assessing the safety of structures after an event.

Forensic analysis of damaged structures to understand residual capacity and develop protocols for rapid assessment: The ultimate goal of this project would be to develop an inspection protocol/checklist to be followed in assessing structural safety, which can be done rapidly in times of crisis. The first step might be to compile a report or synthesis of "bridge morphology." This should be a complete listing of all bridge failures, collapses, and demolition. The purpose is to obtain a broad view of what can happen to a bridge. The next study would expand our interest to include major damage to bridges. After determining the most likely incidents, conduct an analytical and experimental study of damaged structures to determine their remaining capacity and to understand how and why the damage occurred. The study will require a literature search of the subject and an exhaustive study of reports on past damaging events. Then it will be necessary to develop analytical and laboratory models of the damaged parts of the structures for further testing. It may also be possible to obtain portions of old or damaged bridges for the laboratory tests. Once the testing is done, develop new protocols for assessing damage and remaining strength.

Inspection techniques for rapid safety assessment of damaged structures: In times of crisis, being able to rapidly determine the residual strength of structural members is crucial. This study would develop nondestructive evaluation techniques/capabilities to assist the structural engineer in determining the residual capacity of damaged structures.

Damage assessment guide for extreme events: This study would produce a field guide based on the results of previous studies for the assessment of structures for damage from extreme event loadings. It would develop guidance on emergency stabilization analysis; failure investigation;

material strength evaluation; and determination of which areas are safe and which areas need to be demolished, and which methods should be used for demolition.

Repair and Restoration

Goal: Develop better repair and restoration techniques to restore a structure to its original capacity.

Emergency repair procedures: Studies on this will require an idea of the types and levels of damage that are expected. This would have to be done as part of system analysis and design, probably as a study (or studies) under assessment of current bridge and tunnel designs for structural vulnerability to multiple hazards. There would be studies to determine the damage expected under various single hazards. The next step would be to predict the damage caused by two or more simultaneous events. This information could be used as a starting point in identifying and/or developing emergency repair procedures. Once we know the nature of the damage to be expected, repairs can be developed. As a start, this would involve shoring, temporary spans, precast or prefabricated members, and also repairs to damaged members that have retained considerable strength and are salvageable. The study should also find other ways to repair or replace damaged members and keep traffic flowing. Maintenance and protection of traffic should be an integral part of these studies.

Accelerated repair and restoration techniques for reconstruction after an event: These studies will complement and flesh out the emergency repair procedures covered above. Accelerated methods are a must for emergency repair procedures. In fact, except for routine maintenance, most repair procedures should be accelerated since they usually interfere with traffic or are executed under difficult physical conditions. Application and monitoring of innovative concepts for repair or replacement complete this study. Considering the demands in terms of working rapidly and fixing weakened members, developing and deploying innovative procedures is another must.

SECTION 6: SUMMARY

Protecting critical infrastructure against terrorist events is a need imposed on us by the events of September 11, 2001. Although the transportation community has always responded to natural hazards (and there are procedures in place to design for and handle these), managing for terrorist events presents a new challenge. FHWA has been proactive by reaching out to stakeholders to identify critical gaps and needs. This has been accomplished through several forums as presented in this report. The input provided by experts in the field of bridge engineering and others has been evaluated and a program has been proposed to design highway bridges and tunnels for security. There are studies underway addressing some of these needs, but most of these are narrow in scope and additional studies need to be conducted to close the gaps. It is recognized that additional high-priority projects may surface as research is completed and that identification of critical needs is a dynamic process.

APPENDIX A

RESEARCH NEEDS FROM NEEDS ASSESSMENT

Risk and Vulnerability Assessment

1. Because the ways in which a terrorist could potentially attack a bridge are numerous and highly varied, and the possibilities are limitless if the bounds of reason and probability are not applied, we must first have a threat definition. The results of a decade of effort by our country, as well as others, in defining the most probable terrorist threats against military structures, embassies, etc., can be used as a starting point for defining threats against bridges.
2. Cost-benefit and risk-assessment methodologies must be developed to economically address all terrorist threats against bridges, as there are many different bridge types and different degrees of damage depending on the bridge type.
3. Develop methodology to conduct consequence analysis (e.g., how to assess the possible consequences of a truck bomb exploding near a critical member on the bridge).
4. Vulnerability prediction tools: Once the loadings, damage mechanisms, and residual strengths of bridge elements are better understood, these results should be incorporated into new and/or existing vulnerability prediction tools.
5. It is proposed that a research effort be performed to establish guidelines for evaluating the vulnerability of transportation tunnels to terrorist threats. The guidelines will be developed from the latest state of the technology with regard to tunnel structural damage from explosions, the propagation of blast pressures and thermal effects in tunnel systems, and fire or blast control and mitigation techniques for underground facilities. The guidelines will be provided in a user-friendly, AT-Planner type computer format, and will allow users to:
6. Determine which tunnels are structurally vulnerable to terrorist attacks and which are not.
7. Threat vs. risk definition: Prior to any detailed efforts to define specific bridge vulnerabilities, specific terrorist threats and the probability of occurrence (i.e., risk) for each threat must be defined. Definitions of the most probable threats are required in terms of type, size, and location on the bridge. Threat types considered should, at a minimum, include vehicle or boat bombs, hand-carried bombs (e.g., briefcase, etc.), precision cutting charges (i.e., shaped charges), kinetic energy threats such as vehicle or airplane impact, and fire. The size of the threat can range from a hand-cartable weight all the way up to that carried in a tractor-trailer vehicle.
8. Guidelines for evaluating credible threats (e.g., is a truck bomb probable/credible?, is a shaped charge probable/credible?, is a ship/barge impact probable/credible?, etc.).

Design and Analysis

9. Impact dampening designs.

10. Bridge types and design features less prone to damage from terrorist attack.
11. Develop more nonlinear inelastic design approaches, taking advantage of structural ductility.
12. Better protection of piers against impact and/or blast loadings.
13. Use of more continuous structures.
14. Use of redundancy in structures.
15. Deterrent effects of layered countermeasures.
16. Additional knowledge and understanding of the influence of member geometry on local performance under blast conditions.
17. Additional knowledge and understanding of the influence of the structural system on global performance under blast conditions.
18. Although for large suspension cables the likelihood is low that the cable could be severed or even lose enough capacity to cause bridge collapse, the cable size (which is related to bridge size) below which this would be a very serious problem needs to be defined. The vulnerability of the smaller diameter intermediate cable is also unknown. Another concern for cable hangers is the number of successive hangers that would need to be removed in order to induce a spontaneous "unzipping" of the remaining hangers because of load redistribution.
19. Development of guides for proper protection of end anchorages of suspension cables.
20. Simple threat vs. required standoff distances (i.e., vulnerability curves) are required to aid engineers in mitigating the threat of bomb blasts on structures both above and below the decks of bridges. Vulnerability curves should also be developed for the typical truss elements of a through truss or through arch bridge.
21. The intermediate supports (piers and bents) for any type of bridge span could be vulnerable to blast loadings (vehicle or boat bombs). The smaller column portion of bents will be the most vulnerable to lateral loadings from adjacent blasts. Again, vulnerability curves need to be developed for typical piers to allow engineers to design appropriate standoff devices to mitigate these threats.
22. In the specific area of bridges, the U.S. Army Corps of Engineers' Engineer Research and Development Center (ERDC) recently developed a computer code, entitled Bridge Analysis System (BAS), for smart targeting of bridges with precision-guided, air-to-surface weapons. The BAS development effort included a thorough search of international literature in the areas of weapon effects against bridges and structural response of bridges subjected to blast and fragment loadings. A large amount of bridge attack/damage data was also collected from recent U.S. military actions, including Iraq, Bosnia, and Serbia. A key part of the BAS is a weapon effects database, which is weapon specific and predicts the level of damage imparted to the bridge structural elements based on the weapon's impact conditions and the location on the bridge. The database was developed at the ERDC using dynamic finite element (FE) analyses of steel and reinforced-concrete structural elements (beams and girders) impacted by a combination of blast and fragment loadings. The methodology developed for the definition and application of combined blast and fragment loadings on FE models was very innovative and represents the state of the art in this area.

23. Simplified analytical techniques are insufficient to properly study the structural vulnerability of cable-supported towers. Detailed analyses should be accomplished using hydrocodes to predict the complex blast loadings, coupled with FE models of the towers with all in situ loadings present.
24. Development of guidelines for sizing members to enhance bridge performance under blast conditions.
25. Design of concrete structures using fracture mechanics principles rather than static loading criteria.
26. Determination of design safety factors appropriate for dynamic and blast loading applications.
27. Better protection of the bearings, shoes, etc., of suspension and cable-stayed bridges.
28. The application of systems engineering and the availability of advanced technologies have made it clear that earthquake hazard mitigation effects should be considered in combination with other natural and manmade disasters. By the same logic, highway systems are interconnected with other modes of transportation. It may be useful for FHWA to point out that advanced technologies from FHWA can be extended to facilitate the intermodal transportation needs of the public.
29. Damage and strength reduction to generic structural elements: Many of the technology shortfalls involve explosive loadings on key structural elements of specific bridge types (e.g., decks, girders, piers, etc.). Many of these elements are similar in nature and carefully planned studies of generic elements can address many bridge types at once. These studies should encompass a carefully planned combination of simplified analyses, detailed analyses, and actual testing. The residual load capacity of the damaged elements should also be studied in a similar manner. As controlled explosive tests on bridge elements have been almost non-existent in the past, testing should be a priority, even if only done on a limited basis.
30. Structural loadings from terrorist threats: The loadings from blast-type threats must be defined in terms of airblast magnitudes and durations, and fragment densities and velocities. Kinetic energy impactors must be defined in terms of mass, velocity, and impact locations. These definitions may be accomplished through a combination of full- and reduced-scale field tests and analytical modeling. Existing predictive computer codes for military weapons can then be modified to include terrorist weapons.
31. Vulnerability of specific bridge types: As the research progresses, it will probably become apparent that some bridge types, such as truss bridges, need to be studied as a complete structural system rather than as individual structural components. These studies will include detailed analytical calculations using the results from tasks 2 and 3 above and may involve limited field tests of actual bridge structures. As field tests of entire bridge structures will be very costly, these will only be done as a last resort to analytical modeling.
32. Identify critical locations for possible placement of explosive charges.
33. Determine the potential extent and type of damage as a function of the tunnel design and the explosive charge size.

34. Determine the airblast and vehicle damage levels that would occur at any point in the tunnel as a function of the threat (charge size and location).
35. Identify possible protection methods to reduce casualties/damage.

Prevention, Detection, and Surveillance

36. Threat reduction/mitigation measures: As the research progresses, the true vulnerability of specific bridges and bridge elements will become apparent. This will allow for the development of threat reduction/mitigation measures such as standoff devices, intrusion prevention doors, fragment protection panels for beams and cables, blast-resistant design detailing, etc.
37. Consider intrusion detection monitoring for major structures.
38. Detection and warning systems to prevent dangerous cargo from getting into tunnels.
39. Classify major structures and coordinate with the Department of Defense to monitor by satellite.
40. Identify bridge surveillance and security technologies.
41. Use of global information system (GIS) technology to safeguard critical structures, record current road network conditions, etc.
42. Global positioning system (GPS)-based systems: Increased reliance on GPS-based systems for communication with many transportation systems in the United States could compromise traveler safety in the event of signal disruption. That is the conclusion of a study by the Volpe Transportation Center in a report entitled *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System* (www.navcen.uscg.gov/news/FinalReport-v4.6.pdf). GPS technology can be adversely affected by atmospheric effects, signal blockages from structures, interference from other signals, and deliberate disruptions. Although of primary concern to the aviation industry, other modes of transportation are increasingly relying on GPS technology for everything from tracking to traffic management. The report recommends that the State DOTs create an awareness of GPS vulnerabilities, improve their backup systems, and install monitoring systems to warn users of interference with GPS signals.
43. Means of protecting traffic control systems from physical and cyber attacks.
44. Real-time chemical sensors.
45. Neutralizing agents and robots that can test areas and perform decontamination.
46. Deterrent effects of tactics to create uncertainty (“curtains of mystery”).
47. Explosive detection systems able to detect a wider range of materials.
48. Means to network and combine sensors into “sensor fusion.”
49. Standoff and accurate field sensors with low rates of false alarms.
50. Development of guidelines for restricting access to critical bridge members.

51. Determine when and how to take mitigative measures – surveillance and intervention (e.g., physical barrier coming up), hardening critical members, limiting truck operations along critical lanes, etc.
52. Provide guidelines for the design of surveillance systems, including the kind of system, location, etc.
53. Detection of dirty bombs in tunnels through the use of sensors. Determine if there is a justifiable need or a practical method for detecting dirty bombs on a continuous basis.
54. Monitoring of structural performance to detect problems and prevent the occurrence of critical situations.
55. Development of an active safety system for critical transportation facilities that could stop a suspect vehicle traveling on a structure.
56. Use of remote-sensing, space-based observation systems to assist in a variety of ways in improving transportation security. Identifying and reducing vulnerabilities through the use of remote-sensing technologies would help security professionals protect our vast transportation system. Our recommendations to DOT call for establishing interoperability standards for remote-sensing transportation information, which will then be used by security officials at the Federal, State, and local levels.
57. Remote sensing is the process of employing electronic cameras or other types of sensors to image a subject or sense its presence and composition at a distance from the subject. A digital camera and a radar detector are both simple forms of remote-sensing technologies. Sensors may be mounted on satellites, aircraft, or on ground-based platforms. For example, the Landsat satellite system, developed by NASA, has been collecting remotely sensed images of the Earth for more than 30 years. A report is available based on a workshop convened at George Washington University by the National Consortium for Safety, Hazards, and Disaster Assessment for Transportation Lifelines (NCRST-H) in order to effectively assist transportation officials to meet the threat of terrorist activities throughout the country. In addition to identifying potential applications for the technology, major barriers were also identified, alerting experts to the need for additional tools to scrutinize these weaknesses.

Post-Event Assessment

58. Improved inspection techniques to assess damage to structures.
59. Rapid determination of structure condition to determine residual stresses in structural members.
60. There are very specific procedures that should be followed any time a tunnel is entered after an internal explosion. First, the air quality must be sampled to ensure that the tunnel is safe to enter without a breathing apparatus. If hazardous gas levels are still high in the tunnel, these must be used. Secondly, the tunnel must be inspected as it is entered for unstable structural damage that could result in injuries from falling debris (hardhats alone are not good enough). The Bureau of Mines has well-defined procedures for re-entries in the mining business. In the case of an explosion in a transportation tunnel, some minimal risks must be accepted in order to reach and rescue any people inside. It is expected that the Bureau of Mines guidelines would cover such rescue operations. Most fire departments should have

similar procedures for entering fire- or explosion-damaged buildings. Since the initial re-entry will require the use of air quality monitors and other equipment, inexpensive handheld radiation detectors could easily be added if there is a suspicion that a dirty bomb might have been used. It is likely that those detonating a dirty bomb have the objective of getting the contaminants dispersed as widely and efficiently as possible and that structural damage is not their primary objective. Thus, the use of such a bomb to also damage a structure would probably be less likely. They would try to put it closer to population concentrations (e.g., downtown, etc.).

Repair and Restoration

61. Rapid repair of damaged structures.
62. Decontamination of large-scale transportation infrastructure. In FHWA-led workshops on security, the difficulty of fully decontaminating large-scale transportation infrastructure arose repeatedly. This was particularly the case with radiological events, where it may not be possible to simply "wash off" surface contamination as would be done with chemical or biological hazards. This may also be a consideration in whether additional detection is necessary to protect bridges and tunnels. In the extreme, it might be necessary to replace (in part or whole) a bridge or tunnel structure that was structurally sound, but which could not be adequately decontaminated. This area needs to be fully explored. The most complex workshop decontamination scenario was a 32-centerline kilometer (20-centerline mile) section of interstate contaminated with a persistent chemical agent. The cost and scale of decontamination was astounding. The attendees could not figure out if the soil outside the shoulders would have to be removed (and replaced) in order to avoid recontamination of the roadway. Firefighters and hazardous materials specialists have never considered anything on this scale.
63. Rapid replacement/repair: Uninterrupted traffic flow is the most important requirement, so we have to focus on the development of efficient procedures/methods (new materials, technology).
64. Material performance.
65. Additional knowledge and understanding is needed in the performance of different materials under different types and magnitudes of blasts.
66. Development of guidelines for material selection to enhance bridge performance under blast conditions.
67. Development of new technology to promote toughness in concrete materials (e.g., micro- and nano-fiber materials) that can inhibit crack propagation from dynamic loading and blast loadings.
68. Determine the effects of radiation exposure on the structural properties of materials used to design our structures.
69. The most promising area for improvement of bridge performance and longevity is new materials. We need new materials and more sophisticated electrical equipment for the future.

70. There is a need to know what are the pressures generated in blasts of ammonium nitrate, dynamite, nitroglycerin, etc., as a function of poundage and distance (radial pressure distribution), and the millisecond duration of such pressures.

Evaluation and Training

71. Integration of critical databases in a GIS format.
72. Institute a Highway Innovative Technology Evaluation Center (HITEC)-type evaluation program for bridge and tunnel security.
73. There could be a course on anti-terrorist measures given to bridge inspectors to specify the areas of vulnerability on a bridge-by-bridge basis. Immediate field action should follow, with a biennial repeat.

Others

74. There is a need to work with other agencies that have been involved with terrorism and the protection of military structures to transfer knowledge to civil structures.

APPENDIX B

RECOMMENDATIONS OF THE BLUE RIBBON PANEL FOR BRIDGE AND TUNNEL SECURITY

A Blue Ribbon Panel (BRP) of bridge and tunnel experts was convened to examine bridge and tunnel security. FHWA's charge to the panel was to "develop short- and long-term strategies for improving the safety and security of the Nation's bridges and tunnels, and to provide guidance to highway infrastructure owner/operators." Its recommendations are recorded in report no. FHWA-IF-03-036, *Recommendations for Bridge and Tunnel Security*, September 2003.[(2)] The intent of the report is to "recommend policies and actions to reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and social-political damage." Toward this end, the BRP makes seven overarching recommendations in three areas: institutional, fiscal, and technical. The report, however, focuses more on the technical recommendations because of the charge that it was given and because of the collective strengths and expertise of the panelists. Summarized below, from the report, are the Overarching Recommendations, followed by more detailed recommendations for R&D that address the near- and long-term design and engineering solutions.

OVERARCHING RECOMMENDATIONS

Institutional Recommendations

1. Interagency Coordination
2. Outreach and Communication Strategies
3. Clarification of Legal Responsibility

Technical Recommendations

4. Technical Expertise – Security solutions should be "engineered" and FHWA, as the Nation's primary federal agency with the necessary engineering expertise, serve as the coordinating agency for prioritizing critical bridges and tunnels and administering program to allocate funds to responsible agencies to meet high priority security needs.
5. Research, Development, and Implementation – Engineering standards do not exist regarding security concerns for bridges and tunnels. Technology should be developed and validated through appropriate R&D initiatives identified herein to address this need.

Fiscal Recommendations

6. New Funding Sources for Bridge/Tunnel Security.
7. Funding Eligibility.

Research and Development Recommendations

The BRP recommends R&D initiatives with a goal of creating "empirically validated computational tools, design methods and hardening technologies to assist in designing for the terrorist attack." The recommendations with short- and long-term elements are directed to FHWA, AASHTO and other government-sponsored research activities, including universities and federal laboratories.

1. Assess performance of critical elements under credible loads (including load reversals)

   Short-term (within the next year):

   - Synthesize current state of knowledge for component properties and modeling

   Long-term (more than one year):

   - Establish the load structure and load interaction
   - Start component experiments; recommend large-scale testing using real materials, components, and connections under comparable strain rates
   - Conduct comparative parameter studies of typical components and materials

2. Validate and calibrate computational methods and modeling with experiments to better understand structural behavior from blast loads

   Short-term (within the next year):

   - Pull together and examine studies and research that have already been conducted on bridge and tunnel elements and components
   - Investigate transferability of seismic design

   Long-term (more than one year):

   - Develop a predictive round robin analysis of actual blast experiments on bridge and tunnel components
   - Test critical components, such as suspender ropes, stay cables, concrete and steel decks, side loads on towers, and box sections, for testing and blast performance

3. Validate and calibrate computational methods and modeling with experiments to better understand structural behavior from thermal loads

   Short-term (within the next year):

   - Pull together and examine studies and research that have already been conducted on bridge and tunnel elements and components

   Long-term (more than one year):

   - Evaluate various mitigation fire effects in tunnels, double deck bridges, and overpass bridges

4. Determine the residual functionality of bridge and tunnel systems and their tolerance for extreme damage

   Short-term (within the next year):

   - Examine bridges and tunnels compromised in wars and after demolition attempts

   Long-term (more than one year):

   - Determine progressive collapse potential of various bridge and tunnel systems

5. Develop mitigation measures and hardening technologies

   Short-term (within the next year):

   - Assess existing hardening technologies and the applicability to bridges and tunnels

   Long-term (more than one year):

   - Develop new materials and new design methodologies

In addition to these R&D recommendations, the BRP suggests AASHTO work with university engineering institutions to develop R&D programs for students and bridge professionals to address security concerns. The panel recommends that DHS work jointly with industry and state and local governments to explore and identify potential technology solutions and standards that will support analysis and afford better and more cost-effective protection against terrorism.

APPENDIX C

RESULTS FROM THE SECURITY WORKSHOP

The product of this workshop was an unstructured and unprioritized collection of gaps in knowledge, understanding, and technology. This represented the collective thinking of a group of knowledgeable and experienced professionals who have been directly engaged in improving the security of the Nation and its highway systems at the operational and policymaking level.

Reducing the Vulnerability of the Nation's Highway Systems

1. Need for a better understanding of the interrelationship and interdependencies of the highway network and other systems.
2. The sharing of sensitive information is perceived as a need that will prevent us from achieving our goal of improved security.
3. Information, methods, and tools for prioritization are needed.
4. Targets need to be identified.
5. Network analysis is lacking.
6. National network vulnerability analysis is lacking.
7. Multi-objective optimization within a vulnerability and security framework is needed.
8. Is it possible to do this by simply tying local networks together?
9. The threat is unknown and hard to quantify in a probabilistic sense. Traditional risk assessment methods are hard to apply.
10. Insider threats and crime also need to be considered. (We have not considered how to reduce the risk of highways being used to help commit crime.)
11. Other critical infrastructure needs to be considered, such as transit.
12. An explicit definition of what is critical infrastructure is needed.
13. Can cargo tracking technology reduce risk?
14. Cost-benefit analysis of vulnerability reduction.
15. Model elements and test them. There is a need to verify models for testing. There are tools, but no clear models, so we need to verify models (cannot go off of computer assumption).
16. Need to contribute to DHS Critical Infrastructure R&D Plan.
17. Specific information on connection details is lacking (connection within a bridge, not the columns) (e.g., 100-year-old steel bridge).
18. National strategy for spending not in place for security infrastructure.

19. Looking at other scenarios other than the common blast scenario (e.g., poison in cargo ship). Other threats need to be considered.
20. Military standards are available as a tool, but are not necessary applicable to highway cases.
21. There is a need for a National Strategy for spending for security.
22. The assumption that a blast is the most likely threat must be challenged.
23. Ask: What are realistic damage states for highway infrastructure? How much damage is tolerable? Where are we vulnerable?
24. In an ideal world, know what is in the carrier (ship, truck). Cargo tracking technology is needed.
25. Risk needs to be considered in the TSL stage.
26. Low-cost changes to new structures need to be reviewed and included in overviews.
27. National local networks need to be tied together. There is much information floating locally; there is no national tie-in to bring it all together.
28. Security threats from inside agencies should be considered.
29. Cost-benefit analysis is necessary.
30. Risks to be considered in early part of design.
31. Ticket checker example. System design for operations strategies. They need to be checked. How often do we check systems in place? Security checks?
32. Fire suppression and analysis are necessary.
33. Research the application of artificial intelligence or other adaptive computational methods and emerging technologies to this aspect of the problem.
34. Information about threats:
    a. Intelligence ration: Getting information to the right people.
35. Validation tools/models for analyzing dynamic failure (blasts, impacts).
36. Probability risk assessment methodology:
    a. Ranking critical infrastructure (assessing it).
    b. Distribution of funds.
    c. Strategies to reduce risk.
37. Physical vulnerability vs. operational vulnerability.
38. Operational vulnerability:
    a. Power grid systems (cause and effect).
39. Design guides/specifications: Ultimate goal is cost-effective measures.
40. Creating a tool to make it more cost-effective.
41. Cost-effective advanced materials (nanotechnology) design solutions.

42. Integrated software tools (integrating different modules for better decisionmaking).
43. Alternative power source (off grid for traffic control purposes).
44. Handling sensitive security information:
    a. Getting it to the right person.
    b. Plans and designs as examples of this information (whether available or not).
    c. Computation/modeling.
    d. Goal: Developmental work protected, but final product is open.
    e. Legislative involvement and impact on changes.
    f. Final product and availability.
45. Biological/radiological sensors.
46. Improve surveillance and monitoring capabilities.
47. Transportation issues:
    a. Broaden our focus.
    b. Transportation funding over model funding.
48. Guidance to be included on the Web (e.g., hazardous materials sites, nuclear sites, bridge locations, defense routes).
49. Is there sufficient knowledge of surge capacity?
50. Smart structures: Can these reduce vulnerability?
51. Rapid post-event assessment methodology in place.
52. Need literature search on what others have done.
53. What are the cross-cutting issues (risk-reduction metrics)?:
    a. Threat, vulnerability, risk assessment, countermeasures against security (risk-reduction metrics).
    b. Interdependencies for infrastructure.
    c. Redundancy (alternative routing/intermodal):
        i. Other options.
        ii. Redundancy reduces criticality and attractiveness.
    d. Collaboration, communications, coordination (i.e., intelligence).
    e. Interoperability.
    f. Analytical tool required.
    g. Security cost tradeoffs (e.g., potholes vs. security).

54. Detection:
    a. Intrusion detection.
    b. Cameras – semi-automated analytical tools to reduce FTE.
    c. Cheap, easy-to-use alternative to current video systems.
    d. Biological/radiation/chemical detection – detect at high speeds.
    e. Institutionalized arrangements for response.
    f. Analytical support tools – synthesizing systems.
    g. Create a system that is not highly dependent on electrical sources.
    h. Broad category of sensing.
    i. Synthesis of existing technology and practices.
    j. Communications between these remote sensors.
55. Deterrence:
    a. Effectiveness of surveillance on deterrence.
    b. Strategies to reduce target value.
    c. Coordination of security risk vis-a-vis other societal values.
    d. Scientific risk – society tools (how much to invest on security).
    e. Effectiveness of physical patterns on deterrence.
56. Defend:
    a. Vulnerabilities:
        i. Suspension bridge towers.
        ii. Bridge cables.
        iii. Through arches.
        iv. Box girders.
        v. Thin-shell underwater tunnels.
    b. Need to identify mitigation strategies and testing methodologies for above.
    c. Materials for defending:
        i. Column wrap.
        ii. High-performance material- fiber reinforced concrete.
        iii. Thermal protection.
        iv. Windows – electromagnetic pulse.
    d. Barrier Effectiveness.
    e. Biological/chemical strategies and technologies.

57. Deny:
    a. Methods to achieve standoff/enforcement (what works for enforcement).
    b. Routing restrictions (access or deny in critical infrastructure).
    c. Strategies to deny access to critical infrastructure.
    d. Parking restrictions (how effective are they?) – inspect, proximity to critical infrastructure and elements.

Reducing the Risk of a Highway System Being Used as a Means to Attack

1. Sensors to detect threat (unauthorized vehicle or cargo).
2. Integration of sensors into a system to detect a threat and perhaps respond.
3. Include institutional process.
4. Technology to deal with data overload.
5. Boiling it down to a green light (data mining).
6. Chain-of-possession system (identify the possessor of freight).
7. Process to share intelligence and data (tied to communications interoperability).
8. Simulation tools to develop and evaluate the above.
9. Testing of actual systems using simulated attack (exercise or drill) at a large scale at the multi-agency level.
10. Sensitivity analysis of frequency of test and exercise.
11. National tracking system:
    a. Integration of State (local) systems at the national level.
    b. Effects of such systems on mobility or congestion.
12. Mobility can spread a biological or radiological agent.
13. Deterrence, or denial of access, if a threat is detected through intelligence (pre-screening).
14. Lack of knowledge of threat. Access to intelligence.
15. Highway ISAC (design and capability analysis).
16. Research on deterrence.
17. Development of new sensors:
    a. PPB sensitivity is here.
    b. MEMS is here.
18. Strategy for deployment of sensors.
19. Reliability of detection studies.
20. Detecting and responding to behavior patterns (pattern recognition).
21. Research on the security benefits of law enforcement (presence and visibility).

22. Other applications of the benefits of this technology for other law enforcement areas.
23. What will public tolerate with regard to infringement on personal liberty?
24. Balance with legitimate movement of explosion, radiation, etc.
25. Legal research into what is our authority to do such things.
26. Tie to permitting systems.
27. Must be coordinated with DHS.
28. Link to intelligence systems.
29. Detect changes in drivers.
30. Technology transfer from other industries that may have better ways of dealing with this.
31. Scalable to the national level.
32. Decision support systems for making investments technologies vs. benefits vs. risk.
33. Fitness for duty (dual benefit).
34. Eyes-on-the-road program – dealing with the data.
35. Reliability of detection study.
36. Linkage to law enforcement system is essential.
37. Research on efficiency and management of a HISAC
38. Proper archiving of data:
    a. Data aspects of the problem.
    b. Data management for security.
39. Coordination with other systems (e.g., Amber Alert).
40. Design of highway to reduce use as a weapon.
41. All aspects need to be considered.
42. Use traffic control systems to thwart an attack.
43. Consider the business interests as well.
44. Possible use of TRANSIMS
45. Need to better understand how the highway system can be used to deliver an attack.
46. Research of targets.
47. Data communications:
    a. Protection at data transmission.
    b. Any control systems.
48. Tracking cargo:
    a. Origin to destination.
    b. Screening for weapons of mass destruction.

49. Route restriction.
50. Managing the flow of hazardous cargo:
    a. Developing analytical tools.
    b. Evaluate the impact of strategies.
51. Developing better screening techniques.
52. Using technology to identify suspiciously operated vehicles.
53. Advanced screening/surveillance.
54. Identifying overheight/overweight vehicles.
55. Establishing rings of security to detect threats.
56. Enabling DOT employees to be more alert (training):
    a. Research to determine the characteristics and attributes of suspicious vehicles/drivers.
57. Identifying human factors research (associated with security aspects/actions in chemical/biological/nuclear/radiological event):
    a. Management.
    b. Employees sent to establish quarantine barriers (looking at other agencies to support).
58. Using bridges as platforms for delivery (study to evaluate citing and design).
59. Research to identify critical node points in our transportation network.
60. Research to provide redundant transportation systems for critical node points.
61. Freight security (applications to borders and tunnels):
    a. Cargo tracking.
    b. Cargo identification.
    c. Anti-hijacking technology (public fleets and private fleets).
    d. Hazardous materials routing.
    e. Vehicle tracking.
62. Traffic surveillance:
    a. Non-typical behavior recognition.
    b. Driver licensing.
    c. Route deviation alerts.
    d. Rapid response techniques.
    e. Remote sensing and tracking (chemical, radiation, biological).
    f. Evaluation of technical solutions and cost.
63. Response and control methodologies.
64. Calibration (resolution of false indications).

65. Threat definition:
    a. What are we designing to prevent?
66. Physical security:
    a. Barrier design guides.
    b. Barrier usage/applications.
    c. Vehicle inspection (visual, sensing).
    d. Routing options (vehicle restrictions).
    e. Rapid threat investigation technology.
    f. Vehicle restrictions.
    g. Access denial.
    h. Rapid removal of vehicles.
67. Evaluation of hardening vs. policing.
68. Tunnel ventilation control and detection systems.
69. Surveillance:
    a. Effectiveness of highway watch.
    b. Terrorist screening of driver's license applications.
70. TWIC requirements at key construction sites/critical factors.
71. Alternatives to standard national security clearance procedure.

Improving the Utility of the Highway Systems to Respond to and Recover From an Attack

1. Role of transportation in a biohazard situation? Traffic control paradigm?
2. Linkage to modeling and simulation.
3. Modeling in advance of an incident.
4. Real-time modeling capability.
5. Decontamination: How to do it? (biological and radiological).
6. Decontaminate vehicles?
7. Exploration of how intelligent transportation systems (ITS) get applied in response and recovery.
8. Capacity of system under extreme situations (emergencies). Reverse directions, etc.
9. Basic highway engineering questions.
10. Linkage to other infrastructure systems (e.g., cell phone systems): How do we do it?
11. Role playing/people simulation: How bad does a situation have to be before an emergency declaration is made? What types of decisions are people willing to make?
12. What other infrastructures could take down the transportation system (e.g., electric grid)?

13. Develop studies on how long it would take to evacuate a city: Evacuation modeling is a gap. Basic behavior information is missing. Some behavior is counterintuitive. Some behavior is contrary to governmental guidance.
14. Taken off of modeling of hurricane evacuations.
15. Dealing with an unplanned evacuation.
16. Pass through in medians (guidance, number, etc.) break the barriers.
17. Understanding what is involved in decontamination.
18. Research into materials that are more tolerant of decontamination.
19. Effective communication with people in vehicles.
20. Basic research in disaster communication.
21. Dealing with pedestrians in an emergency situation.
22. Focus on moving people not just vehicles (linkage to other modes).
23. Traffic officers might not be available.
24. Assumptions need to be changed.
25. Public awareness of routes (public education/preparedness).
26. Optimal decisionmaking tools:
    a. War games.
    b. Simulation.
    c. Lines of authority (changes in laws needed?) – Federal/State/local.
27. Specific roles/responsibility/authority defined and refined through simulation (role playing).
28. Research into rapid recovery, repair, etc.
29. Sensors for real-time analysis and decisionmaking (is the bridge safe to use or not?).
30. Possible need to understand military mobilization needs in today's world.
31. Dealing with emergencies in rural areas.
32. Modeling of the national system lead – interdependency again
33. Research needs to include deployment plan considering the capability of users. Need to train potential users.
34. Identify capabilities needed to respond and use tool.
35. Ultimate effects/constraints to response and recovery.
36. Rapid recovery of ITS infrastructure.
37. Standards for redundancy and reliability of ITS/traffic control systems. Possible implications for design. Back in service in a short time.
38. Standards for systems redundancy (possible implications for design).
39. Dual use must be a basic guiding principle.

40. Include response and recovery to routine events.
41. Research of technology in support of National Incident Management System.
42. Identification processes for key personnel to enter an area in the event of an attack.
43. Clearly developed policy and implementation guidelines for agencies in the event of an attack for tool development.
44. Communication interoperability (SAFECOM):
    a. Voice and data communications, standards, and architecture between effective parties as needed for security event.
45. Identification of alternative routes:
    a. Enhancement of the Strategic Highway Network (STRAHNET).
46. An all-hazards approach in dealing with security issues.
47. Forensics experts (national pool).
48. Quick analysis needed to avert other attacks.
49. Identification of organization to develop tools, use the developed tools, conduct analysis, and provide results.
50. Develop alternative evacuation strategies and plans:
    a. Local.
    b. Regional.
51. Post-event assessment (consistent data-gathering protocol lessons learned).
52. Response planning for an event.
53. Rapid recovery (e.g., rapid replacement of structures (short-term, long-term)).
54. Enhanced traffic monitoring network.
55. Alternative power supply.
56. Evacuation rerouting techniques:
    a. Reversible lanes.
    b. Movable traffic barriers.
57. Medical evacuation planning.
58. Identification and isolation of the hazard.
59. Planning for multiple attacks.
60. Regional coordination through multi-jurisdictional areas.
61. Rapid assessment.
62. Improvement of system use in response and recovery:
    a. Need for rapid repair options materials.

b. Maximizing short-term lane.

c. Emergency lane clearance.

d. Proper amount of system redundancy.

e. Communications (what?, to whom?).

63. Response planning:

a. Human factors in emergency situations: What can you expect?

b. Ability of current network tools to model human behavior under stress.

c. User needs assessment during emergencies (do current models reflect the needs?).

d. What are the data needs for modeling response options?

64. Chemical/biological/radiation cleanup:

a. Structural capacity of damaged critical infrastructure.

b. Tools to access roadway incidents in terms of security implications.

c. Response strategies for DOT employees.

d. Literature search on response to natural disasters and an evaluation of the implications for response preparedness for State and local DOTs.

65. International border implications regarding emergency response and recovery at borders:

a. Jurisdictional issues.

b. Federal roles in developing possible plans.

66. National incident command systems as a requirement for DOT.

67. Coordination of the transportation requirements of special response teams (urban search and rescue) (management training) under national response plan (interdependency).

68. Special structural load-carrying capabilities (analytical techniques).

69. Communications procedures.

70. Legal agreements.

71. Secure communications needs and systems for use in emergency situations. (Federal-Federal, Federal-State, State-State, etc.).

REFERENCES

1. Office of Science and Technology Policy, Executive Office of the President, and the Science and Technology Directorate, Department of Homeland Security, *The National Plan for Research and Development in Support of Critical Infrastructure Protection*, Washington, DC, 2004.
2. Federal Highway Administration, *Recommendations for Bridge and Tunnel Security*, Blue Ribbon Panel Report, Report No. FHWA-IF-03-036, Washington, DC, September 2003.