U.S. Department
of Transportation
Federal Highway
Administration

Recommendations for Bridge and Tunnel Security



Requested by: The American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force

Prepared by: The Blue Ribbon Panel on Bridge and Tunnel Security

SEPTEMBER 2003

U.S. Department
of Transportation

Federal Highway Administration

Recommendations for Bridge and Tunnel Security

Requested by: The American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force

Prepared by: The Blue Ribbon Panel on Bridge and Tunnel Security

SEPTEMBER 2003

Acknowledgments

This report was requested by the American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force and the Federal Highway Administration (FHWA). The work was authored by the Blue Ribbon Panel on Bridge and Tunnel Security, which included James E. Roberts, P.E. (Chair), Dr. John M. Kulicki, P.E. (Vice Chair), Dwight A. Beranek, Joseph M. Englot, Dr. John W. Fisher, P.E., Henry Hungerbeeler, Dr. Jeremy Isenberg, Dr. Frieder Seible, Kenneth Stinson, Dr. Man Chung Tang, and Kary Witt. Sponsor liaisons included James D. Cooper, P.E., and Steven L. Ernst, P.E., representing FHWA, and Dr. Anthony R. Kane, Paul V. Liles, Jr., P.E., and Mary Lou Ralls, P.E., representing AASHTO. Science Applications International Corporation provided technical support to the Blue Ribbon Panel on Bridge and Tunnel Security under a contract with the National Cooperative Highway Research Program (NCHRP).

Foreword

A note from the American Association of State Highway and Transportation Officials and the Federal Highway Administration:

The Blue Ribbon Panel on Bridge and Tunnel Security was formed from renowned engineering experts who generously contributed their time, without compensation, to guide government leaders, infrastructure owners, and the engineering community on how to improve the security of bridges and tunnels. Infrastructure owners are faced with new and largely unexpected challenges to provide physical security against terrorists' attacks on their critical structures. The panel's initiative and collective wisdom reflected in this report will help America meet these challenges.

Table of Contents

Executive Summary

Terrorism against American citizens and assets is real and growing.[1] The number and intensity of domestic and international terrorist events, along with the September 11, 2001, attacks, change the way Americans think and live. Terrorists attack targets where human casualties and economic consequences are likely to be substantial. Transportation and related assets are attractive terrorist targets because of their accessibility and potential impact on human lives and economic activity.[2] Al Qaeda and other terrorist groups are perceived to be unyielding, tenacious, and patient. An Al Qaeda terrorist training manual captured in England contains goals that included missions for "gathering information about the enemy and blasting and destroying bridges leading into and out of cities."[3] In a similar vein, as a Caltrans-funded Bay Area Security Enhancement Project neared completion, a captured Al-Qaeda leader revealed "a bridge in San Francisco or San Mateo was on a list of possible targets for the terrorist network."[4]

The highway infrastructure has vulnerabilities, which must be addressed.

This is important enough to be a matter of national security policy.

Improvements in homeland security must address improvements to critical bridges and tunnels.

A Blue Ribbon Panel (BRP) of bridge and tunnel experts from professional practice, academia, federal and state agencies, and toll authorities convened to examine bridge and tunnel security and to develop strategies and practices for deterring, disrupting, and mitigating potential attacks. The BRP, sponsored jointly by the Federal Highway Administration (FHWA) and the American Association of State Highway and Transportation Officials (AASHTO), acknowledges that the nation's bridges and tunnels are vulnerable to terrorist attacks. The intent of this paper is to recommend policies and actions to reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and socio-political damage.

The success and safety of the transportation system, combined with the perceived number of parallel routes, can lead to the conclusion that the transportation system is so robust that it is not susceptible to significant disruption by terrorist attack. In the opinion of the BRP members, this conclusion is incorrect. In many parts of the country, the transportation system is straining to keep up with the current demands of society and the economy. The actions of terrorists can impose critical damage to some bridges, and, with explosive forces, exert loads that exceed those for which components are currently being designed. Worse yet, in some cases, the loads can be in the opposite direction of the conventional design loads.

---

1 A report compiled by the Transactional Records Access Clearinghouse (TRAC) from the Federal Bureau of Investigation (FBI) budget reports, budget submissions, and Congressional Research Service reports shows FBI terrorism investigations growing by nearly 5 percent between fiscal year (FY) 1997 and FY 2000 and anti-terrorism funding growing by 25 percent between FY 2000 and FY 2002. These increases are a direct reflection of both growth in and concerns about domestic and international terrorism. TRAC is a data gathering, data research, and data distribution organization associated with Syracuse University. See http://trac.syr.edu/ for more information.

2 Dan Hartman, TSA, briefed the BRP on January 27, 2003, in San Francisco and noted the following with respect to transportation system vulnerabilities: (1) highways, bridges, tunnels, trains, and subways are readily accessible; (2) most fixed transportation infrastructure lies unguarded; (3) transportation infrastructure presents prime opportunities for terrorist attacks; and (4) a small, directed force can inflict serious injury, tremendous damage.

3 Texas DOT Project No. 0-4569, Phase 1 (Literature Review and Work Plan), *Executive Summary*, August 15, 2002.

4 "Anti-Terrorist Security Network Almost Done on Bay Area Bridges and Tunnels," *The San Jose Mercury News*, March 25, 2003.

The nation's highway system has vulnerabilities, which must be addressed. This is important enough to be a matter of national security policy.

Among the 600,000 bridges in the United States, preliminary studies indicate that there are approximately 1,000 where substantial casualties, economic disruption, and other societal ramifications would result from isolated attacks.[5] Additionally, the U.S. transportation system includes 337 highway tunnels and 211 transit tunnels; many are located beneath bodies of water, and many have limited alternative routes due to geographic constraints.[6] The BRP recommends prioritization of these bridge and tunnel assets, followed by risk assessment as a guide for allocating federal and state funds to address security concerns, and then implementation of cost-effective operational security measures and engineering design standards to reduce the vulnerability of high priority bridges and tunnels to terrorist attacks.

After considering the nature of the bridge and tunnel components of the highway system and lessons learned from natural disasters, the effects of transportation-related consequences of the September 11th attack, and the recent barge collision in Oklahoma, the panel has determined that loss of a critical bridge or tunnel at one of the numerous "choke points" in the highway system could result in hundreds or thousands of casualties, billions of dollars worth of direct reconstruction costs, and even greater socioeconomic costs.

Improvements in homeland security must address improvements to critical bridges and tunnels.

In the judgment of the BRP, the ordinary cost of construction to replace a major long-span bridge or tunnel on a busy interstate highway corridor in the United States may be $1.75 billion. Experience in reconstruction following major earthquakes suggests that expediting replacement can double the cost of construction. Program costs may double this figure again. The hundreds of fatalities that may occur, possible environmental consequences, and the fact that the site would be a crime scene under investigation, further compound recovery and replacement. During the five years estimated for reconstruction, the socioeconomic loss to the region resulting from losing as many as 14 Interstate highway lanes for an extended period is many times the replacement cost of the facility. Finally, revenue from toll facilities lost through a terrorist attack might dramatically affect the viability of an agency or toll authority.

Although past attempts at quantifying the total cost of a bridge or tunnel outage from natural disasters have not yielded widely accepted results, the BRP believes that loss of a critical bridge or tunnel could exceed $10 billion. A concerted attack on two or more facilities would result in a synergy where the total cost would be more than the sum of individual costs,

---

[5] The estimate of 1,000 critical bridges is based on information presented in *National Needs Assessment for Ensuring Transportation, Infrastructure Security: Preliminary Estimate*, NCHRP Project 20-59(5), prepared by Parsons Brinckerhoff and SAIC, June 2002.

[6] *Development of a Tunnel Management System – Phase I Report*, prepared by Gannett Fleming for the Federal Highway Administration and the Federal Transit Administration under contract # DTFH61-01-C-00067, March 2003.

especially when regional socioeconomic consequences are considered.[7] Moreover, the regional economic consequences of a major coordinated terrorist attack on multiple facilities are almost inestimable. The September 11, 2001, attacks on the World Trade Centers resulted in significant job losses in the area:

> Since the high water mark of 2000, Manhattan has lost some 85,000 jobs, approximately 28,000 of which were related to firm relocations from Manhattan and the remaining 57,000 to recession-related cutbacks and secondary employment losses triggered by the disaster. At least one third of the job loss, or 30,000 jobs, were in finance and insurance, followed by another 20,000 in services.[8]

The attacks also affected tourism:

> The events of September 11th have had a tremendous impact on the City's visitor market. The decline in over five million visitors to 32 million in 2001 (returning to 1996-1997 levels) can be attributed in part to the weakening economy and concerns over security, and in part to the loss of significant Downtown sites.[9]

Eighty-five percent of the commuters in Lower Manhattan use public transit because the number of private automobiles cannot be accommodated downtown. As a result of the September 11, 2001, attack, the PATH commuter rail line and station were rendered unusable. The line carried 67,000 passengers each weekday to Lower Manhattan and was closed for about two years. This was a major factor in the relocation of 103 firms, 1.1 million square feet of office space, and 11,700 jobs from Lower Manhattan to New Jersey. This is indicative of what the socioeconomic loss of a major transportation route can be.[10]

With prospects of such losses and related replacement and user costs looming in the aftermath of a successful terrorist attack, the U.S. Congress recognized that terrorism presents risks unlike risks typically encountered by those who own and/or operate assets that are important to our nation's well-being.[11] Typically, asset owners manage risks associated with natural hazards using well developed risk assessment methods based on mature occurrence models and actuarial loss data that allow them to make informed trade-off decisions among mitigation alternatives and facility insurance. Unlike the case of natural hazards, we are in the dawn of an era in which asset owners feel overwhelmed by uncertainties about the occurrence and potential costs of terrorist attacks and about their legal responsibilities to protect the users of their facilities.

---

[7] The White House Report, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, acknowledges the close relationship between the nation's transportation infrastructure and other segments of the economy: "Interdependencies exist between transportation and nearly every other sector of the economy. Consequently, a threat to the transportation sector may impact other industries that rely on it. Threat information affecting transportation modes must be adequately addressed through communication and coordination among multiple parties who use or rely on these systems."

[8] *Market Analysis for Site Plan Options – Phase One Summary Report (Draft)*, prepared for the Port Authority of New York and New Jersey and the Lower Manhattan Development Corporation by Beyer Blinder Belle and Parsons Brinckerhoff, August 28, 2002, p. 3.16.

[9] Ibid., p. 3.19.

[10] Ibid., multiple pages.

[11] See the preamble to PL 107-297, the Terrorism Risk Insurance Act of 2002, enacted November 26, 2002, in which the unique risks associated with acts of terrorism are acknowledged and temporary financial compensation to insured parties is proposed as a means of contributing to the stabilization of the U.S. economy in a time of national crisis, while the financial services industry develops the systems, mechanisms, products, and programs necessary to create a viable financial services market for private terrorism risk insurance.

It is therefore imperative to identify critical transportation infrastructure, particularly bridges and tunnels, and to provide strategic guidance for investing in countermeasures and risk mitigation strategies. In the case of bridges and tunnels of regional or national significance, the federal government is the funding source of last resort for recovery operations and to restore capability in the event of terrorist attacks. Significant investment to prevent or reduce the consequences of such attacks may well be justified as an alternative to the high cost of response and recovery and subsequent socioeconomic damage.

Overarching Recommendations

The BRP makes the following seven overarching recommendations to accomplish the overall goal of reducing the vulnerability of bridges and tunnels to terrorist attacks. These recommendations fall into three areas: institutional, fiscal, and technical. Recommendations in the fiscal and institutional areas are prerequisites to effective implementation of recommendations in the technical area. These overarching recommendations are as follows:

Institutional Recommendations

- *Interogency Coordinotion.* Recognizing the importance of both operational and engineered solutions and the expertise that exists within the owner/operator community, it is vital that FHWA, AASHTO, Transportation Security Administration (TSA), and other highway transportation stakeholders collaborate to ensure that assessment methodologies and security solutions meet stakeholder needs.
- *Outreach and Communication Strotegies.* FHWA and AASHTO, in partnership with other organizations, should disseminate information about bridge and tunnel security and cost-effective countermeasures to decision makers, facility owners/operators, designers, and elected officials.
- *Clarification of Legol Responsibility.* FHWA should seek to clarify the legal position of state Departments of Transportation (DOTs) and public transportation authorities with respect to their responsibility to act on the indications of risk studies for their facilities.

Fiscal Recommendations

New Funding Sources for Bridge/Tunnel Security. Bridge and tunnel security issues should be addressed with new funding provided beyond and outside of current federal-aid highway funding sources.

Funding Eligibility. To address the need for flexibility to fund critical structures on a programmatic basis, Title 23, Sections 144 and 133, should be amended to allow expenditures for cost-effective strategies for bridge security, as was done for seismic retrofitting. This change should allow federal funding for critical structures without regard to deficiency as currently defined.

Technical Recommendations

Technical Expertise. Security solutions should be "engineered" and FHWA, as the nation's primary federal agency with the necessary engineering expertise, should collaborate with the TSA in its effort to prioritize critical bridges and tunnels and to administer fund allocation to responsible agencies to meet high priority security needs.

Research, Development, and Implementation. Engineering standards do not exist regarding security concerns for bridges and tunnels. Technology should be developed and validated through appropriate research and development (R&D) initiatives identified here to address this need.

These seven overarching recommendations form the backbone of the BRP's perception of bridge and tunnel security requirements. Although the Panel believes that the fiscal and institutional recommendations offered above are essential to cost-effective bridge and tunnel security enhancement, the primary focus of this report is on the technical recommendations, reflecting both the primary objective of this effort and the collective strengths and expertise of the panelists. These technical recommendations include methods for identifying critical bridges and tunnels, operational security measures that employ effective security procedures and available technology, engineering and design approaches for reducing the vulnerability of critical infrastructure, and research and development agenda to gain a greater understanding of structural responses to attacks and countermeasures to avoid or mitigate potential negative consequences.

1. Background, Panel Membership, and Charge

Following the September 11, 2001, attacks, bridge and highway infrastructure engineers face new and largely unexpected challenges relating to the physical security of critical structures against terrorists attacks. Although the September 11th attacks targeted buildings, threats against bridges and tunnels and other highway infrastructure in various parts of the United States have heightened awareness and concern. Bridge and highway engineers are being asked to assess the vulnerability of structures and to identify means for reducing this vulnerability.

In response to this need, the American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force sponsored the preparation of a guide to assist transportation professionals as they identify critical highway assets and take action to reduce their vulnerability.[12] Further, the U.S. Army Corps of Engineers (USACE) has long considered how to make key structures more resilient against enemy attack. Additionally, to develop and transfer knowledge rapidly within the bridge community to improve structure protection against attack, a series of workshops was conducted in early 2003 under the National Cooperative Highway Research Program (NCHRP) Project 20-59(2).

In order to provide guidance to bridge owners, the Federal Highway Administrator appointed members to the Federal Highway Administration (FHWA)/AASHTO Blue Ribbon Panel (BRP) on bridge and tunnel security. Support for this initiative was provided at the request of the AASHTO Transportation Security Task Force.

The following are the members of the BRP:

- Mr. James E. Roberts, BRP Chair, Consulting Bridge Engineer, Imbsen and Associates, Inc. Dr. John M. Kulicki, BRP Vice Chair, President/CEO and Chief Engineer, Modjeski and Masters
- Mr. Dwight Beranek, Deputy Director of Military Programs, U.S. Army Corps of Engineers
- Mr. Joseph M. Englot, Assistant Chief Engineer/Design, Port Authority of New York and New Jersey
- Dr. John W. Fisher, Professor Emeritus, Lehigh University
- Mr. Henry Hungerbeeler, Director, Missouri Department of Transportation, and Chair, AASHTO Transportation Security Task Force
- Dr. Jeremy Isenberg, President and CEO, Weidlinger Associates, Inc.
- Dr. Frieder Seible, Dean, Jacobs School of Engineering, University of California at San Diego

[12] *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* prepared for AASHTO by Science Applications International Corporation, under NCHRP Project 20-7/151B, May 2002. AASHTO plans to refine and update this guide in 2004 to reflect more recent information and to include an economic impact tool that will assist states in dentifying the most cost-effective vulnerability mitigation strategies.

- Mr. Kenneth E. Stinson, Chairman and CEO, Peter Kiewit Sons, Inc.
- Dr. Man Chung Tang, Chairman of the Board and Technical Director, T.Y. Lin International
- Mr. Kary Witt, Bridge Manager and Deputy General Manager, Golden Gate Bridge, Highway and Transportation District

FHWA's charge to the panel was as follows:

> ***Develop short- and long-term strategies for improving the safety and security of the nation's bridges and tunnels, and provide guidance to highway infrastructure owners/operators.***

The panel's objective was to apply its collective experience and knowledge about structural design, structural integrity, and environmental stress and strain to new ways of examining how critical bridges and tunnels can be protected against potential terrorist attacks.

The panel met four times to identify and clarify issues, develop and evaluate potential solutions, and formulate and refine recommendations for improving bridge and tunnel security. The recommendations presented in this report include recommendations on actions that can be taken either by bridge and tunnel owners and operators or by FHWA and other state and federal agencies that will result in improved security and reduced vulnerabilities for critical bridges and tunnels.

2. Blue Ribbon Panel Approach

2.1 Overall Strategy for Bridge and Tunnel Security — "The Bigger Picture"

Bridge and tunnel security, like security for any infrastructure asset, includes a broad range of issues that must be addressed to ensure that adequate measures are taken to protect the asset and the people and goods that utilize the asset. Table 1 shows the bridge and tunnel security issues considered by the panel organized into topical areas. Several of the topics and related issues are of general interest and apply to all transportation infrastructure; others relate more directly to bridges and tunnels. For example, the "management and operational practices" issues apply to most infrastructure assets (transportation and otherwise), as do "information security," "mobilization and response," and "recovery" issues. However, issues that fall within the "planning, design, and engineering" area may be unique to bridges and tunnels and require special solutions that go beyond what might be needed to reduce the vulnerability and improve the security of other infrastructure assets.

Table 1. Bridge and Tunnel Security Issues

Key Topics in Infrastructure Security	Specific Issues
1. Foundations for Policy	• Criteria Establishing Investment Priorities • Institutional Continuity
2. Planning, Design, and Engineering	• Design Review for Secure Structures • Research and Development (R&D) Needed to Support "Design for Security" • Design Criteria • Design Specifications
3. Management and Operational Practices	• Best Practices • Practice Review • Institutional Relationships • Preparedness • Personnel and Vehicle Security • Communication/Outreach
4. Information Security	• Procurement Practices • Information Security
5. Mobilization ("Notice") and Response ("Trans-event")	• Threat Warning • Early Response • Initial Response
6. Recovery (Post-event)	• Damage Assessment

The panel's special expertise is in the area of bridge and tunnel planning, design, and engineering; therefore, the primary focus of recommendations contained in this report addresses near- and long-term design and engineering solutions to bridge and tunnel vulnerabilities.

2.2 Framework for Planning, Design, and Engineering

During its initial meeting, the BRP established a framework for addressing bridge and tunnel security. This framework includes the following elements considered essential to developing sound recommendations for reducing bridge and tunnel vulnerability to terrorist attacks:

- A means of identifying "critical" bridges and tunnels, through prioritization and risk assessment
- Designation of the specific threats to be considered "terrorist attacks" (e.g., to eliminate military attacks with precision guided munitions)
- Determination of the kinds of damage of concern (e.g., structural, contamination)
- Countermeasures considered in response to potential threats and damage
- The adequacy of current knowledge and available codes and specifications to enable design professionals to retrofit existing facilities and design hardened new facilities

2.3 Prioritization and Risk Assessment

A standardized, objective process is needed to identify those bridges and tunnels that are most likely to be targeted for a terrorist attack and the cost-effective projects to thwart the attack. *Prioritization* is the process of identifying the likely targets; *risk assessment* is the process by which methods of defeating the attack will be selected. Both are needed to establish a financial scope (i.e., to determine how much money it costs to deter and provide defense compared to the facility and social cost from the loss) and to allocate available funds appropriately.

Therefore, the BRP advocates both of the following:

- A *prioritization method* that could be based on subjective or empirical criteria and is accessible to a wide range of interested parties,[13, 14]
- A *risk assessment method* that is based on rigorous engineering and mathematical principles accessible to experts and modeled after the methodology used for seismic studies by building on the risk methodology summarized in Section 4 of this report

2.4 Threats

Assessment of vulnerability requires consideration of the means of inflicting damage to a facility, that is, the threat or threats. The analogy to the conventional design process is the

[13] These criteria should represent a consensus among stakeholders as to what makes a facility "important" in terms of an agency's mission. In his April 1, 2003, testimony before the National Commission on Terrorist Attacks Upon the United States, G.L. Dillingham of the General Accounting Office states "A criticality assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy. The assessment provides a basis for identifying which structures or processes are relatively more important to protect from attack. As such it helps managers to determine operational requirements and to target resources to the highest priorities, while reducing the potential for targeting resources to lower priorities."

[14] The BRP recognizes that the *AASHTO Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* is the current methodology and acknowledges it as a starting point for prioritizing bridges and tunnels; however, prioritization of bridges and tunnels requires more specific criteria and methods, such as those recommended later in this report.

identification of the design loads. Effective countermeasures and associated costs cannot be developed without this assessment just as the amount of steel and concrete needed in a bridge or tunnel cannot be calculated if the loads are not known. The following types of threats are considered by the BRP:[15]

- Low-tech and high-tech conventional explosives (e.g., shape charges)
- Explosively formed penetrating devices (EFP, kinetic energy penetrators)
- Low-tech, hand-held cutting devices
- Truck size/barge size conventional explosives
- Chemical/biological agents released in tunnels
- Incendiary conventional explosives
- HAZMAT release in tunnels
- Intentional ramming via ship or barge

2.5 Damage

For the purposes of this report, the consequences of attack expressed as damage to bridges and tunnels that are of concern are as follows:

- Threats to the integrity of the structure (e.g., resulting in replacement of the facility or major repairs)
- Damage that inhibits the structure's functionality for an extended period of time, such as closure of the facility for 30 days or more
- Contamination of a tunnel resulting in extended closure or loss of functionality
- Catastrophic failure resulting from an attack based on the threats described above

2.6 Countermeasures

If the process of prioritization and risk assessment leads to the conclusion that a given bridge or tunnel must be made more secure, there are a variety of countermeasures that can be used singly or in combination to reduce attractiveness and/or vulnerability, or to reduce consequences if an attack occurs. Countermeasures are often grouped into actions or technologies to deter attack, deny access, detect presence, defend the facility, or design structural hardening to minimize consequences to an accepted level. Because of its expertise, the BRP dealt primarily with the last category of countermeasures. The panel's focus does not imply that other strategies for deterring, detecting and denying, or defending are not valid options. In many cases, risk assessment as recommended here will lead to the conclusion that one or more of the non-design countermeasures is the most appropriate

[15] Recognized experts from USACE presented background information on many of these types of threats to augment the knowledge within the panel.

and cost-effective solution for a given facility. There are relatively mature technologies and strategies currently available for implementation. Application of these countermeasures still requires enabling funding but not necessarily the research and analysis commitment necessary to develop and implement effective design countermeasures. For completeness, a list of possible low-cost immediate actions to increase security exposure has been collected from several such sources and is appended here.[16]

2.7 Codes and Specifications

Considering consequences focuses attention on the ability to deal with the structural engineering ramifications. Some engineering guidance is available within the Department of Defense (DOD). However, the panel has determined that current design codes and specifications leave much to be desired in terms of how to employ hardening design, how to quantify blast-related demands, and how to determine the capacity of components exposed to high-pressure transients.

Research agenda to fill in the gaps in current understanding of phenomena and response have been developed and are contained in Section 4. Given this basic knowledge, practical comprehensive design guidance and specifications can be developed as outlined here.

[16] See Appendix B for a list of commonly used operational security measures that fall into this category of countermeasures.

3. Overarching Recommendations

The seven overarching recommendations fall into three categories: institutional, fiscal, and technical. Recommendations in the first two areas are prerequisites to effective implementation of recommendations in the third area. These recommendations are as follows:

3.1 Institutional Recommendations[17]

- *Interagency Coordination.* Recognizing the importance of both operational and engineered solutions and the expertise that exists within the owner/operator community, FHWA, AASHTO, Transportation Security Administration (TSA), and other highway transportation stakeholders should collaborate to ensure that assessment methodologies and security solutions meet stakeholder needs.
- *Outreach and Communication Strategies.* FHWA and AASHTO, in partnership with other organizations, should disseminate information (e.g., case studies, guidebooks, funding needs) about bridge and tunnel security and cost-effective countermeasures to decision-makers (federal agency leadership, e.g., DHS, U.S. Department of Transportation [USDOT], USACE), facility owners/operators, (state/local DOTs and authorities), designers (state DOTs, industry, academics), and elected officials (Congress, governors, mayors). Relationships already established through The Infrastructure Security Partnership (TISP) should be leveraged to facilitate outreach and implementation.
- *Clarification of Legal Responsibility.* FHWA should seek to clarify the legal position of state DOTs and public transportation authorities with respect to their responsibility to act on the indications of risk studies for their facilities. State DOTs should be informed of legal precedent that will guide them in evaluating risk to facilities without becoming vulnerable to victims' claims that knowledge was not translated into action soon enough.

3.2 Fiscal Recommendations

- *New Funding Sources for Bridge/Tunnel Security.* Bridge and tunnel security issues should be addressed with new funding provided beyond and outside of current federal-aid highway funding sources. These funds should come from the Department of Homeland Security (DHS). Transportation agencies are unable to keep up with national needs with current funding as identified in FHWA's Conditions and Performance Report.

[17] Since September 2001, federal, state, and local surface transportation agencies and the private sector have begun rethinking roles and responsibilities for transportation security. One challenge to achieving national preparedness hinges on the federal government's ability to form effective partnerships among entities that implement security measures at the local level. Effective, well-coordinated partnerships require identifying roles and responsibilities; developing effective, collaborative relationships with local and regional transportation, emergency management, and law enforcement agencies; agreeing on performance-based standards that describe desired outcomes; testing procedures that implement roles and responsibilities; and sharing intelligence information. *Testimony of G.L. Dillingham, General Accounting Office, before the National Commission on Terrorist Attacks Upon the United States, April 1, 2003.*

Many states receive one-fourth to one-third of needed funding to preserve existing infrastructure. The trust fund must not be diverted.[18]

- *Funding Eligibility.* To address the need for flexibility to fund critical structures on a programmatic basis, Title 23, Sections 144 and 133, should be amended to allow expenditures for cost-effective strategies for bridge security, as was done for seismic retrofitting. This change should allow federal funds to be expended on critical structures without regard to deficiency as currently defined.

3.3 Technical Recommendations

- *Technical Expertise.* Security solutions should be "engineered," and FHWA, as the nation's primary federal agency with the necessary engineering expertise, should collaborate with the TSA in its effort to prioritize critical bridges and tunnels and to administer fund allocation to responsible agencies to meet high priority security needs. This collaborative activity should produce a consistent risk model and cost-benefit analysis approach.
- *Research, Development, and Implementation.* Engineering standards do not exist regarding security concerns for bridges and tunnels. Technology (e.g., algorithms, materials, design tools, construction methods) should be developed and validated through appropriate R&D initiatives identified here to address this need. R&D efforts should lead to development of methods and standards to guide countermeasures design and implementation. Efforts should be taken to build on the knowledge base available from DOD and other agencies. The goal is to develop these tools and then adopt them into the appropriate AASHTO and other specifications.

These seven overarching recommendations form the backbone of the BRP's thinking regarding bridge and tunnel security. Although the panel believes that the fiscal and institutional recommendations offered above are essential to cost-effective bridge and tunnel security enhancement, the primary focus of this report is on the technical recommendations, reflecting both the primary objective of this effort and the collective strengths and expertise of the panelists. These technical recommendations include methods for identifying critical bridges and tunnels, operational security measures, engineering and design approaches for reducing the vulnerability of critical infrastructure, and related research and development needs.

[18] In considering the federal government's role in meeting long-term funding challenges, several issues will need to be addressed beyond determining who should pay for the security enhancements and to what extent the agency functions should be funded. An important consideration is, which criteria are most appropriate for distributing federal funds? The chief criteria considered have been ridership level, population, identified vulnerabilities, and criticality of assets. Another important consideration, as we reported in September 2002, is, which federal policy instruments — grants, loan guarantees, tax incentives, or partnerships — are most appropriate to motivate or mandate other levels of government or the private sector to help address security concerns? Finally, it will be important to consider how to allocate funds between competing needs and to measure whether we are achieving the increased security benefits envisioned. Testimony of G.L. Dillingham, General Accounting Office, before the National Commission on Terrorist Attacks Upon the United States, April 1, 2003.rity benefits envisioned. *Testimony of G.L. Dillingham, General Accounting Office, before the National Commission on Terrorist Attacks Upon the United States, April 1, 2003.*

All of the recommendations are to FHWA and AASHTO unless otherwise noted. The panel recognizes that several recommendations require collaboration with other federal agencies, in particular the Department of Homeland Security (DHS), and the panel encourages DHS to consider these recommendations. Recommendations that address policy foundations and institutional continuity are presented in Section 4. Technical design, engineering, and R&D recommendations are presented in Section 5.

4. Policy Foundations And Institutional Continuity

4.1 Foundations for Policy and Planning

Potential choices for dealing with risks associated with bridges and tunnels, in general terms, include the following:

- Acceptance (no action)
- Mitigation (retrofit, operational changes, add redundant facilities)
- Transfer (insurance, self-insurance, or other financial instruments)

The criteria for making choices related to these facilities will be applied at the national, regional, or local level. Owners of facilities are using existing technology and information to enhance the security of critical assets by diverting program funds away from maintenance and construction until federal funds are available specifically for security. The goal of policy is to develop and encourage the use of consistent prioritization and risk assessment methods leading to actions that will enhance bridge and tunnel security.

Assessment

In the near-term, the primary basis for prioritization and risk assessment is the National Bridge Inventory System (NBIS) maintained by FHWA. NBIS contains data about bridges (no tunnel data), including location, structure type, span characteristics, average daily traffic volume, military significance, and other use-related information. This data can help inform the decision process for selecting high priority bridges for near-term security countermeasures.

Recommendations

Near-term (3-6 months):

1. FHWA should engage AASHTO, through its standing committee structure, informed by current information such as studies, reports, and briefings, to review and comment on proposed funding programs to improve bridge/tunnel security against terrorist attacks. This activity should be supported through AASHTO, NCHRP, FHWA, or other national funding sources to offset travel and other meeting expenses.
2. FHWA should summarize the current status of critical bridges and tunnels identified through previous studies.

Mid-term (6-12 months):

1. FHWA should collaborate with the TSA and other stakeholders to develop a bridge and tunnel prioritization process based on the methodology outlined in Section 5.
2. FHWA should develop guidelines for applying the prioritization approach, including illustrative examples and technical assistance.
3. FHWA should issue a FHWA Technical Advisory on how to implement available and applicable technology and procedures to enhance bridge and tunnel security, including potential funding sources, technical contacts, streamlined procurement, and other information.

Long-term (12-18 months):

1. FHWA should encourage application (via solicitation/response cycle) and refinement of processes through a centralized "clearinghouse" where results are used to improve processes.

4.2 Institutional Continuity

Continuity is necessary to ensure implementation and periodic evaluation by a recognized, credible, representative, and relevant national organization empowered to deal with Security Sensitive Information (SSI) and promulgate policies and specifications. A forum for information exchange among entities responsible for surface transportation security would help to provide this continuity.

The Transportation Security Administration (TSA) is developing risk assessment methodologies and countermeasures for all transportation modes. The BRP encourages TSA to leverage FHWA and state DOT and facility owner/operator experience in vulnerability assessment and security measures so that TSA methodologies reflect the needs of DOTs and facility owner/operators as well as the homeland security needs of the nation.

Assessment

The panel recognizes that policy guidance for transportation security will be formulated as a collaborative effort among TSA, FHWA, AASHTO, and other highway transportation stakeholders. The panel recognizes that AASHTO is the most appropriate organization for implementing security policy within the highway bridge and tunnel community.

Recommendations

Near-term (3-6 months):

1. Recognizing the importance of both operational and engineered solutions and the expertise that exists within the owner/operator community, FHWA, AASHTO, TSA, and other highway transportation stakeholders should collaborate to ensure that assessment methodologies and security solutions meet stakeholder needs.
2. It is assumed that TSA will promulgate top-level performance-based design guidance. Detailed implementation strategies should be developed by FHWA, AASHTO, and other sources of technical expertise.
3. With respect to highway bridges and tunnels, an AASHTO entity is the most appropriate organization to address security issues.[19]
4. Recognizing that many facilities have dual use, and working with TSA, a dialogue should be established between the AASHTO Technical Committee and similar entities representing rail organizations (AAR) and transit providers (APTA) responsible for similar structures and operations.

[19] At its first meeting, the BRP recommended that the AASHTO Standing Committee on Bridges and Structures (SCOBS) form a new permanent Technical Committee on Bridge and Tunnel Security. This recommendation was acted upon immediately. Technical Committee T-1 was to have its first meeting at the June 2003 SCOBS meeting. The panel encourages the AASHTO SCOBS to engage other bridge and tunnel stakeholders in its activities.

5. Planning, Design, and Engineering Recommendations

Because of its heterogeneity in size and operations and the multitude of owners and operators nationwide, the transportation infrastructure network in the United States is highly resilient, flexible, and responsive.[14] Unfortunately, the sector is fractionated and regulated by multiple jurisdictions at state, federal, and sometimes local levels. The size and pervasive nature of the U.S. transportation infrastructure poses significant protection challenges.[20] However, these protection challenges can be mitigated through technical collaboration and coordination.

5.1 Review and Prioritization Process

A process is necessary for prioritizing all bridges and tunnels with respect to their vulnerability in terms of their criticality of the ability to deter, deny, detect, delay, and defend against terrorist attacks. In addition, a risk assessment model must be developed as a framework for evaluating alternatives for thwarting attack.

Several agencies have developed methods for identifying and prioritizing critical transportation assets, and these methods share many commonalities. The prioritization procedure outlined in the AASHTO's methodology uses a set of *critical asset factors* to identify assets that are important to achieving an agency's mission. Next, the AASHTO methodology assesses the *vulnerability* of these critical assets to terrorist attack based on *target attractiveness* (potential casualties and symbolic value); *accessibility* (access controls and physical security); and *expected damage* (including environmental hazards).[21] The TSA approach determines relative risk as a function of *relative target attractiveness* (an assessment of the target's importance and consequences); *relative likelihood of occurrence* (an assessment by TSA Intelligence of the likelihood of occurrence, as compared to the other scenarios); and *vulnerability* (a measure of how likely the terrorist is to achieve the threatening act given that an attempt is made). Relative risk is re-calculated based upon the implementation of a suite of countermeasures, including the implementation of people, procedures, and/or technology to reduce vulnerability.[22]

---

[20] Transportation choke points (e.g., bridges and tunnels, inter-modal terminals, border crossings, and highway interchanges) present unique protection challenges. Overall understanding of infrastructure choke points is limited. Common criteria for identifying critical choke points are therefore difficult to establish. We must undertake a comprehensive, systematic effort to identify key assets, particularly those whose destruction or disruption would entail significant public health and safety consequences or significant economic impact.... A major reason for this lack of synchronization within the sector is a paucity of funds to promote communication among industry members and facilitate cooperation for joint protection planning efforts. As a result, the sector as a whole has neither a coherent picture of industry-wide risks, nor a set of appropriate security criteria on which to baseline its protection planning efforts, such as what conditions constitute threats for the sector, or standards for infrastructure protection or threat reduction. The sector's diverse and widely distributed constituency complicates this situation. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The Office of the United States White House, Washington D.C., 2003.

[21] *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, prepared for AASHTO by Science Applications International Corporation, under NCHRP Project 20-7/151B, May 2002.

[22] Briefing to the FHWA/AASHTO Blue Ribbon Panel on Bridge and Tunnel Security presented by Tom Reilly, Transportation Security Administration, Department of Homeland Security, March 27, 2003.

Assessment

The panel considered and rejected several options:

1. Do nothing, which the panel found unacceptable under post-September 11th threats.
2. Have states conduct their own assessment using prioritization and risk assessment methodologies of their own choice. This is unacceptable because federal funds will be required to meet countermeasure needs and the federal government will need a common, uniform, and consistently applied methodology to compare needs.
3. The federal government conducts assessment throughout all the states. This is unacceptable because it does not take into account states' operating needs, and the states are much more knowledgeable in assessing their own bridge and tunnel assets.

Because national prioritization of funding will be required, the process of evaluating proposals to enhance bridge and tunnel security must be a joint effort by federal and state agencies and other owners and operators.

The large number of bridges (600,000) and tunnels (500) lends itself to a two-tier approach: prioritization and risk assessment. The first tier, prioritization, is typically most efficiently done in two steps. The first step is a data-driven approach, such as that used by the Texas Department of Transportation (TxDOT), for ranking bridges using common criteria.[23] The National Bridge Inventory (NBI) provides much of the data needed for this step. In the second step of prioritization, additional data comes from owners and operators familiar with specific characteristics of the facilities and the services they provide. In this first tier ranking, prioritization of bridges and tunnels should be based on characteristics such as the following:

- Potential for mass casualty based on Average Daily Traffic (ADT) and associated peak occupancies
- Criticality to emergency evacuation and response to emergencies
- Military or defense mobilization
- Alternative routes with adequate available capacity
- Potential for extensive media exposure and public reaction; symbolic value (to what extent does the facility represent ideals and values that are important to the American public, also visual symbolism, e.g., "signature bridges")
- Mixed-use bridges and tunnels where highway and rail are co-located
- Potential for collateral damage (land, marine, rail), including collateral property and utilities
- Maximum single span length as it relates to the time required to replace the facility

[23] "Transportation Security Update," briefing presentation by Tom Rummel, P.E., Project Development Section, Bridge Division, Texas Department of Transportation, February 2003.

- Commercial vehicle vs. passenger vehicle mix and volume as a surrogate for economic impact
- Bridge or tunnel dimensions (as a surrogate for replacement time/cost)
- Significance of revenue streams (e.g., tolls, fares) associated with the facility[24]
- Bridges and tunnels at international border crossings

The second tier is a risk assessment of high priority bridges taken from the first tier (prioritization) to determine vulnerabilities and evaluate countermeasures to deter attack and/or mitigate damages. The risk, R, to the facility is determined following an approach similar to that developed for seismic retrofit and can be expressed as follows:[25]

$$R = O \times V \times I$$

where,

O = Occurrence: In the general form of the risk equation, this factor is hazard oriented and will change with the nature of the hazard. In the context of this report, the occurrence factor approximates the *likelihood* that terrorists will attack the asset. It includes target attractiveness (from the perspective of the threat), level of security, access to the site, publicity if attacked, and the number of prior threats. Input into this factor typically comes from the law enforcement and intelligence communities familiar with threat and operational security measures.

V = Vulnerability: In the general form of the risk equation, vulnerability is an indication of how much the facility or population would be *damaged* or *destroyed* based on the structural response to a particular hazard. In the context of this report, vulnerability is the likely damage resulting from various terrorist threats (weapon type and location). It is a measure of expected damage, outcome of the event, expected casualties, and loss of use, all features of the facility itself. Input into this factor typically comes from engineering analysis and expertise.

I = Importance: Importance is a characteristic of the facility, not the hazard. In principle, importance is the same for any hazard. Importance is an indication of *consequences* to the region or nation in the event the facility is destroyed or unavailable. Is the facility on an evacuation or military mobilization route; is it likely to be used by first responders to emergencies; what is its historic and associated significance; what is its peak occupancy? Input into this factor typically comes from owners, operators, users, and beneficiaries of the facilities, often governmental sources, and will use factors similar to those used in the first tier prioritization.

[24] Revenue streams associated with facilities may not make them attractive targets, but their loss could seriously affect the economic viability of entities that depend on revenue derived from them to maintain continuity of operations.

[25] The proposed approach is consistent with the approach suggested by the TSA and with approaches currently used by entities that have completed or are performing risk assessments.

This formula properly expresses the interaction among the three factors. Dominant factors magnify risk; negligible factors diminish it. Other formulas, such as models that add the factors, fail to account for their interactive effects. For example, in the absence of a threat ('O'=0), the risk should be zero as this model provides; additive models would have a residual risk. In the multiplicative model, eliminating any one factor to zero (or near zero) reduces the risk to near zero (e.g., low importance leads to low risk regardless of other factors).

The countermeasures that reduce the risk associated with an asset may be designed to reduce the occurrence factor (e.g., make the asset less accessible); the vulnerability factor (e.g., harden the facility to reduce damage); or the importance factor (e.g., add redundant facilities to reduce dependence on the asset).

A case study illustrating application of this risk assessment approach to bridges and tunnels is provided in Appendix C.

Recommendations

The panel recommends a state identification and prioritization of bridges and tunnels, followed by a federal re-prioritization for federal funding based on the following:

Near-term (3-6 months):

1. FHWA determines and promulgates a methodology for reviewing bridges and tunnels with respect to their risk and vulnerability in terms of their ability to detect, deny, delay, and defend against terrorist attacks. Methodologies that may be considered should be developed and include the *AASHTO Guide for Highway Vulnerability Assessment*, the Texas DOT methodology, and others.
2. Using methodology promulgated by the FHWA similar to that described above, states should prioritize their bridges and tunnels and submit prioritized lists of their most critical bridges and tunnels to FHWA.
3. FHWA/AASHTO should oversee the development of an immediate, near-, and mid-term cost-benefit methodology based on probabilistic risk assessment for implementing countermeasures. Within the framework of probabilistic risk assessment of the kind that has been adopted for seismic retrofit programs, consideration should be given to existing methodologies.

Mid-term (6-12 months):

1. FHWA takes states' priority lists of critical bridges and tunnels and develops a national list of critical bridges and tunnels.
2. States use the risk assessment methodology to develop a countermeasures plan using a cost-benefit ratio as a metric and provide costs for implementing countermeasures for each of their critical bridges and tunnels to FHWA.

Long-term (12-18 months):

1. FHWA, in collaboration with DHS/TSA and other agencies, seeks new appropriations from Congress to implement a national bridge and tunnel countermeasure program. FHWA begins allocating funds to the highest priority bridges and tunnels as identified by the states and other owners/operators in accordance with accepted risk assessment methodologies.
2. Non-state DOT bridge and tunnel owners begin implementing countermeasures consistent with federal security standards using appropriate funding sources, including federal sources where applicable.
3. FHWA in coordination with AASHTO develops and implements modifications to existing bridge and tunnel inspection programs to evaluate conformance to federal security standards.
4. States implement countermeasures with funding as available. One source recommends an initial sum of at least $1.5 billion to address near-term security measures.[26]

5.2 Research and Development

Assessment

The analysis of current structural components and their behavior to blast loads is recognized by the panel as key to understanding the proper and most efficient ways to mitigate terrorist attacks through structural design and retrofit. Table 2 lists key structural bridge components that the panel considered.

Table 2. Critical Bridge Components

Suspension and Cable-Stayed Bridges	Truss Bridges	Arch Bridges
• Suspender ropes, stay cables • Tower leg • Main cable • Orthotropic steel deck • Reinforced and prestressed bridge decks • Cable saddle • Approach structures • Connections • Anchorage • Piers	• Suspended span hangers • Continuous and cantilever hold-down anchorages • Compression chords or diagonals • Connections • Decks • Piers	• Tension-tie • Connections • Decks • Piers **Multi-girder/Freeway Overpass Bridges** • Decks • Connections • Piers

[26] *National Needs Assessment for Ensuring Transportation Infrastructure Security*, prepared by Douglas B. Ham and Stephen Lockwood, Parsons Brinckerhoff, for the American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force as part of NCHRP Project 20-59, Task 5, October 2002.

Recommendations

The goal of the R&D initiatives recommended here is to create empirically validated computational tools, design methods, and hardening technologies to assist in "designing for the terrorist attack." The recommendations have one or more short-term and long-term elements and all are directed to FHWA, AASHTO, and other government-sponsored research activities, including universities and federal laboratories. Additionally, these five recommendations are interrelated and interdependent and should be pursued simultaneously:

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.[27]

5.3 Design Criteria

Assessment

The acceptability of a threat is the criterion for determining how to design for the threat. Performance level design is based stating assumptions and setting expectations and goals. These factors could include threats, casualties, damage, and recovery. To set a performance level design criteria, the design process must first be described, taking into account the potential threats to the existing or planned bridge or tunnel. The panel recommends that bridge and tunnel owners and operators use the following six-step process:[28]

1. Use previously determined *"R,"* the risk for each bridge or tunnel, whether existing or planned, determined using the $R = OVI$ model.

   a. *Determine Threats.* There are several potential threats that exist. The first and most serious is a precision demolition attack. If carried out, this attack will destroy or seriously damage the bridge or tunnel. Therefore, this threat must be mitigated so that it will not be allowed to happen. Other threats to consider are conventional explosives, collision, and fire. Their potential magnitude is presented in Table 3.

[27] One recommendation related to transportation infrastructure is to "harden industry infrastructure against terrorism through technology. DHS will 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." *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The Office of the United States White House, Washington D.C., 2003.

[28] See Appendix C for a case study of the application of this design methodology.

Table 3. Magnitude of Threats

Threat Type	Largest Possible	Highest Probability
Conventional explosives	Truck*: 20,000 lbs Barge: 40,000 lbs	Car bomb**: 500 lbs
Collision to structure (i.e., the size of a vehicle that could collide with a structure)	Truck: 100,000 lbs GVW Water Vessel: depends on waterway	Truck: H-15 Water Vessel: (see AASHTO spec. LRFD on vessel impact)
Fire	Largest existing fuel or propane tank Largest fuel vessel or tanker	Gasoline truck (3S-2) Fuel barge
Chemical/biological HAZMAT	These threats exist; however, the panel is not qualified to quantify them. Therefore, other experts should assess these threats in this way.	

* Largest possible conventional explosive – for a truck, based on largest truck bomb ever detonated internationally by a terrorist act. For a barge, based on the assumption that it is the largest explosive that could pass by unnoticed by current security at place at major waterways.

** The size of an explosive charge that can be concealed within the trunk of an automobile without being visually detected when inspecting the automobile.

b. *Determine the Consequence.* Based on the potential threats to the bridge or tunnel, the owner must decide the potential consequences if carried out.

2. Determine the acceptability of consequences. If the consequences are acceptable, then the owner may decide to do nothing.

3. If the consequences are unacceptable, then one of two options exists:

   a. *Mitigate the Threat.* Generally, these actions can be taken in the short term (3-6 month range). Owners should take measures to lessen the attractiveness or deny access through technology, operational procedures, and physical measures.

   b. *Mitigate the Consequence.* These actions fall into the mid- to long-term time frame. Reduce the damage and resulting loss of life, property, functionality, and economic viability through design, engineering, and operational strategies.

This step in the process requires detailed engineering analysis, vulnerability assessments, and statistical analysis of specific facilities and postulated threats to those facilities.

4. Estimate the cost of mitigating the threat or consequence.

5. Recalculate the *R=OVI* based on the recommended mitigation approach to determine the risk reduction achieved.

   a. Assets that receive a high R score should be categorized as a "high priority" structure. Steps should be taken to mitigate the largest possible threat in this situation. Designs should be performed so that in the event of this threat there would be no irreparable

damage and the structure could return to operable condition in 30 days. Higher probability threats should be designed so that in event of threat there is not loss of service.

b. Assets that receive a low R score should be categorized as a "low priority" structure. The criteria for these structures in the event of the largest possible threat is that total loss is acceptable. The destruction of these low priority assets will not be devastating to the region because of alternative routes, size, economic implications, and socio-political messages. Higher probability threats should be designed so that in the event of threat there is minimal loss of service.

6. Compare the costs and benefits (risk reduction) of varying mitigation combinations and strategies under designated analysis scenarios. In determining the cost and benefits associated with various mitigation strategies and countermeasures, the analysis should include cost related to increased user cost and potential environmental/energy cost effects if the facility were destroyed or seriously damaged.

As an alternative possibility for acceptability criteria guidance, the bridge owner may consider what sort of time frame it can handle for loss of service. For example, if the time frame is 13 days, then the bridge owner can determine what sort of threat type (from car, boat, etc., or size of explosives) could potentially do this damage, and mitigate for this threat.

The recommendations for design criteria are based on various mitigating strategies. Owners have the choice to mitigate the threat (preventing terrorists facility access), mitigate the consequence effect (lessening the effect from an attack), or apply both options.

The following are examples of approaches to ***mitigate threats:***

- Establishing a secure perimeter using physical barriers
- Inspection surveillance, detection and enforcement, closed circuit television (CCTV)
- Visible security presence
- Minimize time on target

The following are examples of approaches to ***mitigate consequences:***

- **Create Standoff Distance.** The first level of mitigating terrorist attacks should be to incorporate sufficient standoff distances from primary structural components. Providing standoff distance is highly recommended. *There are three basic approaches to blast resistant design: increasing standoff distances; structural hardening of members; or higher acceptable levels of risk.* Often, utilizing a percentage of each strategy is optimal.
- **Add Design Redundancy.** Structural systems that provide great redundancy among structural components will help limit collapse in the event of severe structural damage from unpredictable terrorist acts.
- **Hardening/Strengthening the Elements of the Structure.** Structural retrofitting and hardening priority should be assigned to critical elements that are essential to mitigating the extent of collapse. Secondary structural elements should be dealt with to minimize injury and damage.

- **Develop an Accelerated Response and Recovery Plan.** Alternative routes and evacuation plans should be known and established.

Recommendations

FHWA, in collaboration with AASHTO and TSA, should use the countermeasures development and evaluation methods described in this section to assess countermeasure effectiveness. Typical countermeasures to be considered are shown below and in Appendix A. Countermeasures should be ranked and implemented based on the cost-benefit analysis approach described here.

5.4 Technology Development And Dissemination

The overall objectives in the area of technology development and dissemination are to: (1) develop a bridge and tunnel security technical program, including cost estimates and resources; and (2) develop an educational curriculum for students and bridge professionals.

Assessment

The panel has determined that a sufficient body of knowledge exists to assemble an interim structural assessment/design guide based on the following:

- Existing blast software
- Strain-rate based constitutive laws or resistance adjustments
- Ductility/deformation limits
- Existing plastic design of steel and Ultimate Strength Design (USD) of concrete, adjusted as indicated in (1), (2), and (3) above

Recommendations

1. FHWA and AASHTO, in collaboration with the USACE and DHS/TSA and others, collect and synthesize existing information, analyses, and case studies and prepare interim findings to support quantitative analysis of blast effects, structural response, and countermeasures cost-effectiveness. These findings should include points of contact (agencies, firms, and individuals) with specific expertise in bridge and tunnel blast analysis.
2. The panel recommends that AASHTO and FHWA endorse The National Pooled Fund Project, TPF-5(056), *Design of Bridges for Security,* TxDOT Project No. 0-4569, August 15, 2002.
3. The BRP recommends that AASHTO work with university engineering institutions to develop an educational curriculum for students and bridge professionals to address security concerns. AASHTO should consider supporting the "Educational Bridge" program sponsored by the National Society of Professional Engineers (NSPE) in collaboration with TISP though which universities are being encouraged to integrate infrastructure security into their curricula.

6. Recommendations Summary

This section summarizes recommendations made by the BRP. Sub-sections 6.1, 6.2, and 6.3 summarize short-, mid-, and long-term strategies, respectively, for improving bridge and tunnel security. Sub-section 6.4 summarizes design guidance for facility owners/operators to use in mitigating threats to facilities or the consequences of an attack on facilities. Sub-section 6.5 gives the BRP concluding observations and overall recommendations for moving forward in addressing bridge and tunnel security issues.

6.1 *Short-term Strategies* for Improving Bridge and Tunnel Security

Policy and Planning

- FHWA should engage AASHTO, through its standing committee structure, informed by current information (studies, reports, briefings), to review and comment on proposed funding programs to improve bridge/tunnel security against terrorist attacks. This activity should be supported through AASHTO, NCHRP, FHWA, or other national funding sources to offset travel and other meeting expenses.
- FHWA should summarize the current status of critical bridges and tunnels identified through previous studies.

Institutional Continuity

- Recognizing the importance of both operational and engineered solutions and the expertise that exists within the owner/operator community, FHWA, AASHTO, TSA, and other highway transportation stakeholders should collaborate to ensure that assessment methodologies and security solutions meet stakeholder needs.
- It is assumed that TSA will promulgate top-level performance-based design guidance. Detailed implementation strategies should be developed by FHWA, AASHTO, and other sources of technical expertise.
- With respect to highway bridges and tunnels, an AASHTO entity is the most appropriate organization to address security issues.
- Recognizing that many facilities have dual use, and working with TSA, FHWA should establish dialogue between the AASHTO Technical Committee and similar entities representing rail organizations (AAR) and transit providers (APTA) responsible for similar structures and operations.

Review and Prioritization

- FHWA should determine and promulgate a methodology for reviewing bridge and tunnel risks and vulnerabilities with respect to detecting, denying, delaying, and defending against terrorist attacks. FHWA should develop methodologies that may be considered and include the *AASHTO Guide for Highway Vulnerability Assessment*, the Texas DOT methodology, or others.

- Using methodology promulgated by FHWA similar to that described here, states should prioritize their bridges and tunnels and submit prioritized lists of their most critical bridges and tunnels to FHWA.
- FHWA/AASHTO should oversee the development of an immediate, near-, and mid-term cost-benefit methodology based on probabilistic risk assessment for implementing countermeasures. Within the framework of probabilistic risk assessment of the kind that has been adopted for seismic retrofit programs, consideration should be given to existing methodologies.

Research and Development

- FHWA should synthesize the current state of knowledge for component properties and modeling of critical elements under credible loads (including load reversals).
- FHWA should pull together and examine studies and research that have already been conducted on bridge and tunnel elements and components as a first step toward validating and calibrating computational methods and models to understand structural behavior from blast and thermal loads.
- FHWA should investigate transferability of seismic design.
- FHWA, in collaboration with other research partners, should examine bridges and tunnels compromised in wars and after demolition attempts to determine residual functionality of bridge and tunnel systems and their tolerance for extreme damage.
- FHWA should assess existing hardening technologies and their applicability to bridges and tunnels.

Technology Development and Dissemination

- FHWA and AASHTO, in collaboration with the USACE and DHS/TSA and others, should collect and synthesize existing information, analyses, and case studies and prepare interim findings to support quantitative analysis of blast effects, structural response, and countermeasures cost-effectiveness. These findings should include points of contact (agencies, firms, and individuals) with specific expertise in bridge and tunnel blast analysis.
- The panel recommends that AASHTO and FHWA endorse The National Pooled Fund Project, TPF-5(056), *Design of Bridges for Security*, TxDOT Project No. 0-4569, August 15, 2002.
- The BRP recommends that AASHTO work with university engineering institutions to develop an educational curriculum for students and bridge professionals to address security concerns. Consider supporting the "Educational Bridge" program sponsored by NSPE in collaboration with TISP though which universities are being encouraged to integrate infrastructure security into their curricula.

6.2 *Mid-term Strategies* for Improving Bridge and Tunnel Security

Policy and Planning

- FHWA should collaborate with the TSA and other stakeholders to develop a bridge and tunnel prioritization process based on the methodology outlined in Section 5.1.
- FHWA should develop guidelines for applying the prioritization approach, including illustrative examples and technical assistance.
- FHWA should issue an FHWA Technical Advisory on how to implement available and applicable technology and procedures to enhance bridge and tunnel security, including potential funding sources, technical contacts, streamlined procurement, and other information.

Review and Prioritization Process

- FHWA takes states' priority lists of critical bridges and tunnels and develops a national list of critical bridges and tunnels.
- States use the risk assessment methodology to develop a countermeasures plan using cost-benefit ratio as a metric and provide costs for implementing countermeasures for each of their critical bridges and tunnels to FHWA.

6.3 *Long-term Strategies* for Improving Bridge and Tunnel Security

Policy and Planning

- FHWA should encourage application (via solicitation/response cycle) and refinement of prioritization and risk assessment processes through a centralized "clearinghouse" where results are used to improve processes.

Review and Prioritization Process

- FHWA, in collaboration with DHS/TSA and other agencies, seeks new appropriations from Congress to implement a national bridge and tunnel countermeasure program. FHWA begins allocating funds to the highest priority bridges and tunnels as identified by the states and other owners/operators in accordance with accepted risk assessment methodologies.
- Non-state DOT bridge and tunnel owners begin implementing countermeasures consistent with federal security standards using appropriate funding sources, including federal sources where applicable.
- FHWA, in coordination with AASHTO, develops and implements modifications to existing bridge and tunnel inspection programs to evaluate conformance to federal security standards.
- States implement countermeasures with funding as available. One source recommends an initial sum of at least $1.5 billion to address near-term security measures.

Research and Development

- FHWA should establish the load structure and load interaction for the performance of critical elements under credible loads.
- FHWA should start component experiments; recommend large scale testing using real materials, components, and connections under comparable strain rates.
- FHWA should conduct comparative parameter studies of typical components and materials.
- FHWA should develop a predictive round robin analysis of actual blast experiments on bridge and tunnel components.
- FHWA should 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.
- FHWA should evaluate various mitigation fire effects in tunnels, double deck bridges, and overpass bridges.
- FHWA should determine the progressive collapse potential of various bridge and tunnel systems.
- FHWA should develop new materials and new design methodologies.

6.4 Design Criteria/Guidance to Highway Infrastructure Owners/Operators

Mitigate Threats

- Establishment of a secure perimeter using physical barriers
- Inspection surveillance, detection and enforcement, CCTV
- Visible security presence
- Minimized time on target

Mitigate Consequences

- **Create Standoff Distance (Highly Recommended).** The first level of mitigating terrorist attacks should be to incorporate sufficient standoff distances from primary structural components. There are three basic approaches to blast resistant design: increasing standoff distances, structural hardening of members, or higher acceptable levels of risk. Often, utilizing a percentage of each strategy is optimal.
- **Add Design Redundancy.** Structural systems that provide great redundancy among structural components will help limit collapse in the event of severe structural damage from unpredictable terrorist acts.
- **Harden/Strengthen the Elements of the Structure.** Structural retrofitting and hardening priority should be assigned to critical elements that are essential to

mitigating the extent of collapse. Secondary structural elements should be dealt with to minimize injury and damage.

- **Develop an Accelerated Recovery Plan.** Alternative routes and evacuation plans should be known and established.

6.5 Conclusions

- Bridge and tunnel security is important enough to be a matter of national security policy. *The threat is real: attacks at choke points could be devastating.*
- Operational security measures are in place and well known to bridge and tunnel operators who operate "signature" facilities. Additional outreach and education are needed to expand both the body of knowledge about operational procedures and the knowledge and expertise of facility owners and operators. *Site improvements and operational procedures will often prove more cost effective than structural engineering solutions.*
- Bridge and tunnel security require the institutional, technical, and fiscal responses recommended by the BRP in the overarching recommendations. Interagency cooperation is necessary for the development of cost-effective and implementable policies and standards. *New funding must be made available to be able to deal with security issues and still allow for needed maintenance and expansion of the current highway system.*
- Proven tools are needed to set priorities and allocate resources, evaluate "design-for-security" approaches, and assess countermeasure effectiveness. *As big as the problem appears to be, it may be made manageable through prioritization and risk assessment.*
- Research is needed to assess structural responses and to validate and calibrate computational methods and models. *Structural engineering guidance needs to be developed by expanding on work done by DOD through research leading to design guidance.*
- Outreach and education are needed to develop greater awareness and professional capacity to address bridge and tunnel security challenges. *We need trained professionals to understand and meet these challenges.*

Appendix A: Countermeasure Options[29]

The countermeasures listed below are available to bridge and tunnel owners and operators for their use in planning and implementing more effective security practices. The list is provided in the interest of sharing information that may prove helpful to individuals and agencies, but the panel does not recommend specific countermeasures or their application to specific facilities.

Planning and coordination measures

Update the emergency operations plan/crisis management plan to include response and recovery to a terrorist threat involving a bridge. Based on the Federal Emergency Management Agency (FEMA) guidelines, the plan should include the following:

- Concept of operations
- Coordinated response, responsibilities, and liaisons among different departments and agencies
- Sequence of events that should occur for an effective response
- List of potential areas of vulnerability
- Procedures for notification and activation of crisis management teams
- Establishment of a mobile command center with essential communications equipment
- Designated radio frequencies for emergency communications
- Procedures for dealing with bomb threats and suspicious objects
- Evacuation and shutdown procedures
- Identification of emergency evacuation routes and staging areas for response teams
- Measures ensuring safety and security after an incident
- Procedures for restoring service and establishing alternate routes
- Removal plan for damaged equipment and structural elements
- Procedures for issuing information and reassuring the public
- Procedures for dealing with victims and notification of relatives
- Regular updates based on events that identify vulnerabilities in the plan
- Communication and coordination with local, state, and federal law enforcement agencies to obtain terrorism intelligence, training, and technical support

[29] These countermeasure options are from *Design of Bridges for Security: NCHRP Bridge Infrastructure Vulnerability Assessment Workshop*, presented by Capt. David Winget, University of Texas Department of Civil Engineering, February 10, 2003.

- Regular drills, tabletop exercises, no-notice responses, and full-scale simulations aimed at specific objectives to identify problem areas and test response procedures, communication, and coordination
- Plans for rapid debris removal and repairs
- Development of a training plan for maintenance personnel (observant of surroundings and knowing how to deal with suspicious objects)
- Establishment of a security policy

Information control measures

- Review and sanitize websites for potential information that may be beneficial to terrorists. However, removal of data from websites must be balanced with the need for information sharing. For example, information about a specific bridge can be very useful for identifying weaknesses and planning an attack, but general design guidelines and "standard" plans generally provide information that is not directly beneficial to terrorists.
- Establish a common classification system for sensitive information. Implement procedures for the control of sensitive information, including document classification, disposal of sensitive materials, and tracking the distribution of design information to contract tenderers. Establish "need-to-know basis" procedures for the release of vulnerabilities, security measures, emergency response plans, or structural details for specific bridges.

Site layout measures

- Improved lighting with emergency backup (combined with elimination of hiding spaces below)
- Clearing overgrown vegetation to improve lines of sight to critical areas
- Creative landscaping with regular maintenance to increase standoff distance to critical areas
- Elimination of access to critical areas (beneath deck, maintenance rooms with access to cables, etc.)
- Elimination of parking spaces beneath bridges
- Providing pass-through gates in concrete median barriers to enable rerouting of traffic and access for emergency vehicles
- Review of locations of trashcans or other storage areas that could be used to conceal an explosive device, ensure they are not near critical areas

Access control/deterrent measures

- Police patrol and surveillance

- Guards
- Enhanced visibility
- Signs issuing warnings that property is secured and being monitored
- Marked vehicles
- Keyless entry systems
- Exterior and interior intrusion detection systems
- Boundary penetration sensors (below bridge)
- Volumetric motion sensors (for towers, maintenance buildings, inside box girders, etc.)
- Point sensors (critical connections)
- CCTV placed where it cannot be easily damaged or avoided while providing coverage of critical areas (to monitor activity, detect suspicious actions, and identify suspects)
- Incorporation of a higher level of identification procedures and credentials for maintenance personnel, security personnel, and external contractors
- Denied/limited access to critical structural elements (i.e., providing fencing around cable anchors, restricting access to box girders and cable towers, etc.)
- Denied/limited access to inspection platforms
- Physical barriers to protect piers
- Physical barriers to control access to the deck during credible threats to a specific bridge (used in conjunction with random vehicle searches)
- Rapid removal of abandoned vehicles
- No fly zones around critical bridges
- Emergency telephones to report incidents or suspicious activity
- Use of an advanced warning system, including warning signs, lights, horns, and pop-up barricades to restrict access after span failure (manually activated or activated by span failure detectors)

Retrofit Options

- Reinforcing welds and bolted connections to ensure that members reach their full plastic capacity (designed for 120% of connected member capacity to account for strength increases during high-rate straining)
- Using energy absorbing bolts to strengthen connections and reduce deformations
- Adding stiffeners and strengthening lateral bracing on steel members to prevent local buckling before they reach their full plastic capacity

- Designing portions of the deck to "blow out" and create a vent to reduce pressures on the support structure (possibly near the abutments where large pressures build up from confinement effects)
- Adding Carbon Fiber Reinforced Polymer (CFRP) hoop wraps on concrete columns, which can be reinforced with longitudinal wraps, to enhance concrete confinement, increase bending resistance and ductility, and add protection against spalling (can also be used on bents and beams)
- Strengthening the lower portions (or full height) of columns against impacts and localized blast damage by encircling them with a steel casing (connected with high strength bolts and epoxy or a layer of grout)
- Adding lateral bracing to columns to allow them to develop plastic hinges while preventing buckling
- Adding 360-degree pier protection for impacts and standoff distance — possible alternatives include concrete barriers, stationary fender systems, dolphins, rotational bumper systems, or elastomeric energy absorbers
- Restraining sections of the bridge with steel cables to reduce the chance of deck collapse at the supports, including cable supports to keep the deck from separating at the joints and hinge restrainers to hold the deck to the columns (can also be accomplished with high-strength threaded rod restrainers and pipe seat extenders)
- Increasing the size of abutment seats and adding hinge seat extensions under expansion joints to reduce the chance of deck collapse at the supports
- Increasing footing size (possibly combined with adding additional pilings in the ground or using steel tie-down rods to better anchor the footings to the ground) to improve resistance to cratering and large column deformations
- Wrapping the lower portions of cables on cable-stayed bridges and suspension bridges with CFRP or other types of protective armor to protect against damage from blast and fragmentation
- Increasing standoff distance and reducing access to critical elements with structural modifications (extending cable guide pipe length, moving guard rails, etc.)
- Including reinforcing steel on top and bottom faces of girders to increase resistance to uplift forces from blasts that are in the opposite direction from those due to gravity and live loads
- Providing system redundancy to ensure alternate load paths exist (through continuity, strengthening of connections, redundancy in cables and girders, etc.) should a critical structural element fail or become heavily damaged as a result of a terrorist attack
- Strengthening the deck on curved steel trapezoidal girder bridges to ensure that sufficient torsional strength is provided should a portion of the deck be compromised

Threat Level Based Measures

Threat Level to Bridges	Additional Security Measures ("High Priority" – bridges that score a high R)
Severe	• Restrict access with guards, barriers, and vehicle searches • All other measures listed below
High	• Increase frequency of patrols and checks • Conduct unscheduled exercise of emergency response plan • Postpone non-essential maintenance • Coordinate with National Guard or law enforcement for possible closure and vehicle searches when severe level is reached • All other measures listed below
Elevated	• Implement regularly scheduled police patrols • All other measures listed below
Guarded	• Review and update emergency response procedures • Increase frequency of periodic checks of cameras, fences, etc. • All other measures listed below
Low	• Monitor security systems in place (including periodic checks) • Disseminate threat information to personnel • Regularly refine and exercise emergency operations plan • Conduct emergency responder training • Continually update threat and vulnerability assessments

Appendix B: Operational Security Practices

This list of Operational Security Practices was developed during the AASHTO/FHWA BRP initial meeting to ensure that the panel considered the full range of security strategies. Following the initial meeting, the panel focused more narrowly on the design and engineering considerations contained in the body of this report.

Management and Operational Practices

- **Best Practices.** Current and timely exchange of practical information among owners and operators concerning the potential for and counters to terrorist attacks and related matters
- **Practice Review.** Process for reviewing overall security management practices, including personnel policies, training, procedures, and use of technology
- **Institutional Relationships.** Clarification and/or establishment of roles and responsibilities among federal, state, and local entities and effective partnerships for preventing, defeating, and responding to terrorists' attacks
- **Preparedness.** Guidance to owners/operators regarding preparations for responding to terrorists' attacks, including coordination with other federal, state, and local agencies, communication protocols, and equipment interoperability
- **Personnel and Vehicle Security.** Guidance to operators for ensuring that employees, contractors, vendors, visitors, and the vehicles they operate are authorized, verified, and authenticated, as appropriate
- **Communication/Outreach.** Communication strategies for community outreach and coordination of sensitive information (e.g., with other agencies, media, private sector entities)

Information Security

- **Procurement Practices.** Means for procuring security-sensitive technologies without public disclosure and for soliciting construction bids without disclosing security-sensitive design features
- **Information Security.** Means for controlling public access to "as built" drawings and related information

Mobilization ("notice") and Response ("trans-event")

- **Threat Warning.** Means (protocols) for timely notification of owners/operators concerning imminent threats to specific assets
- **Early Response.** Policies and processes for interdicting identified threats, informing/instructing travelers, and evacuating facilities

- **Initial Response.** Policies, process, and technologies needed to execute the preparedness plan in response to terrorists' attacks

Recovery (Post-event)

- **Damage Assessment.** Procedures and technologies that assist in initial assessment of structural damage to the asset to determine the effect of the attack on functionality (e.g., closure, restricted use)
- **Functional Continuity.** Contingency plans for reestablishing asset functionality (including use of available alternatives, emergency repairs)

Appendix C: Case Study in Bridge and Tunnel Risk Assessment

Risk Assessment Approach

This appendix describes the risk assessment method used to help determine how to allocate resources for mitigating the adverse effects of terrorist acts on critical transportation facilities and the occupants of those facilities. Decisions on how best to spend mitigation funds require a rational and systematic risk-based approach that considers, for each facility, the combination of hazard occurrence likelihood, consequences given the occurrence, and socioeconomic importance of the facility. Risk assessment methods for mitigation decisions related to natural hazards are fairly well established. The application of these methods to non-natural hazards (i.e., acts of terrorism) is relatively new. There is no well-established comprehensive procedure that can be used to determine how terrorism mitigation funds should be spent given a finite list of facilities, mitigation alternatives, and agency-defined constraints.

We used a rational and systematic risk assessment method for prioritizing alternatives for mitigating the effects of acts of terrorism. The method makes use of several key sources of information, including the following:

- Prior work in seismic risk assessment for retrofit prioritization (Maroney, 1990; Sheng and Gilbert, 1991; Kim, 1993; Babaei and Hawkins, 1993; Hart Consultant Group et al., 1994; King and Kiremidjian, 1994; Basoz and Kiremidjian, 1995; Audigier et al., 2000)
- DOD procedures for addressing physical threats in facility planning (U.S. Department of Defense, 1994)
- AASHTO Guidelines for highway vulnerability assessment (AASHTO, 2002)
- U.S. Department of Justice state preparedness support program (U.S. Department of Justice, 2000)
- Analytic Hierarchy Process for consensus decision making given multiple attributes (Saaty, 1980)

The risk to a facility due to a man-made hazard is represented as the combination of the following three factors as shown in Figure C-1:

- **Importance Factor (IF).** A measure of the socioeconomic impact of the facility's operation, computed as a weighted combination of the following attributes of the facility:
  - Historical and symbolic importance
  - Replacement value
  - Importance as an emergency evacuation route
  - Importance to the regional economy

  - Importance to the regional transportation network
  - Annual revenue value
  - Criticality of the utilities attached to the facility
  - Military importance
  - Exposed population on or in the facility
- **Occurrence Factor (OF_i).** A measure of the relative probability or likelihood of threat i occurring, computed as a weighted combination of the following:
  - Level of access
  - Level of security
  - Visibility or attractiveness of the facility
  - Level of publicity
  - Number of times the facility has been threatened in the past
- **Vulnerability Factor (VF_i).** A measure of the consequences to the facility and the occupants given the occurrence of threat i, computed as a weighted combination of the following:
  - Expected damage to the asset
  - Expected down-time or closure of the facility
  - Expected number of casualties

Expressed in equation format, the risk score (RS) for a given facility, is written as follows:

$$RS = IF \times \sum [OF_i \times VF_i] \qquad (1)$$

where OF_i, VF_i, and IF are defined as above, and $\sum$ denotes the summation over all considered threats to the facility.

Each of the factors in Equation *(1)* is a number between 0 and 1, computed using a multi-variate utility method. In this method, each factor is computed as the summation of the weighted values (between 0 and 1) of the attributes that define the factor as follows:

$$IF = \sum [W_j \times V_j(X_j)] \qquad (2a)$$

$$OF = \sum [W_j \times V_j(X_j)] \qquad (2b)$$

$$VF = \sum [W_j \times V_j(X_j)] \qquad (2c)$$

where x_j is the value of attribute j (e.g., very high), $v_j(x_j)$ is the function or table that maps x_j to a utility value (between 0 and 1; e.g., very high corresponds to 1), w_j is the weighting factor on attribute j, and $\sum$ denotes the summation over all considered attributes for the factor. See Figure C-1 for a graphical depiction of the above discussion.

The weighting factors used for combining the attributes that make up each of the factors listed above are developed using the pair-wise comparison procedure in the Analytic Hierarchy Process, whereby each member of the decision making group assigns a numerical value to the relative influence of one attribute over another. The scores are averaged and used to compute the weighting factors, which are then reviewed by the group as a whole and revised until all members of the group are satisfied with the results. Figures C-2 through C-4 show the relative weights for the attributes used to compute the Importance Factor, Occurrence Factor, and Vulnerability Factor, respectively.

After the weighting factors have been developed, the risk assessment method proceeds as follows for each facility:

1. Compute the Importance Factor (Equation *(2a)*) by assigning values to the attributes that contribute to the factor
2. Identify vulnerable components of the facility
3. Identify credible threats to each component
4. Compute the Occurrence Factor (Equation *(2b)*) and Vulnerability Factor (Equation *(2c)*) for each threat by assigning values to the attributes that contribute to the two factors
5. Compute the baseline Risk Score (Equation *(1)*) for the facility as a combination of the Importance, Occurrence, and Vulnerability Factors as shown in Figure C-1
6. Identify the mitigation projects for the facility and the threats that will be mitigated
7. For each mitigation project, re-compute the Occurrence and Vulnerability Factors (Equations *(2b)* and *(2c)*) given the presence of the mitigation project, and then re-compute the Risk Score (Equation *(1)*)
8. Rank the mitigation projects in terms of reduction in Risk Score compared to the baseline Risk Score for the facility computed in Step 5

Risk Assessment Results

The result of this risk assessment effort is a ranked list that identifies the benefit of enacting each mitigation project. The costs (in terms of capital expenditure, operation and maintenance, and disruption) were developed in a parallel effort and used with these results in an explicit cost-benefit analysis to identify the final list of mitigation projects to pursue.

Prior to developing the final ranked list of projects based on the cost-benefit comparison, several intermediate results were examined to ensure that the final results would be both rational and practical. For example, Figure C-5 shows the ranking of the eight facilities by Importance Factor. Figures C-6 through C-11 show the breakdown of each facility into the vulnerable components or threat targets.

The final list of mitigation projects, ranked by the ratio of benefit (in terms of reduction in facility Risk Score) to project cost, is given in Table C-1.

Figure C-12 shows the resulting ranked list in a chart format to help illustrate the comparison of mitigation project benefits and costs.

Risk Assessment References

AASHTO, 2002, *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, Prepared by SAIC, Washington, DC.

Audigier, M.A., Kiremidjian, A.S., Chiu, S.S., and King, S.A., 2000, "Risk Analysis of Port Facilities," *Proceedings of the 12th World Conference on Earthquake Engineering*, paper no. 2311.

Babaei, K., and Hawkins, N., 1993, *Bridge Seismic Retrofit Planning Program*, Report WA-RD 217.1, Washington State Department of Transportation, Olympia, WA.

Basoz, N., and Kiremidjian, A.S., 1995, *Prioritization of Bridges for Seismic Retrofitting*, Report No. 114, John Blume Earthquake Engineering Center, Department of Civil Engineering, Stanford University, Stanford, CA.

Hart Consultant Group et al., 1994, *Seismic Risk Decision Analysis for Kaiser Permanente Pasadena, Final Project Report*, Santa Monica, CA.

Kim, S.H., 1993, *A GIS-Based Risk Analysis Approach for Bridges Against Natural Hazards*, Ph.D. Dissertation, Department of Civil Engineering, State University of New York, Buffalo, NY.

King, S.A., and Kiremidjian, A.S., 1994, *Regional Seismic Hazard and Risk Analysis Through Geographic Information Systems, Report No. 111*, John Blume Earthquake Engineering Center, Department of Civil Engineering, Stanford University, Stanford, CA.

Maroney, B., 1990, *CALTRANS Seismic Risk Algorithm for Bridge Structures, Division of Structures*, California Department of Transportation, Sacramento, CA.

Saaty, T.L., 1980, *The Analytic Hierarchy Process*, McGraw-Hill, New York, NY.

Sheng, L.H., and Gilbert, A., 1991, "California Department of Transportation Seismic Retrofit Program: The Prioritization and Screening Process," *Proceedings of the Third U.S. National Conference on Lifeline Earthquake Engineering*, pp. 1110-1119.

U.S. Department of Defense, 1994, TM 5-853/AFMAN 32-1071, Volume 1, Chapter 3, Planning Phase, Washington, DC.

U.S. Department of Justice, 2000, *Fiscal Year 1999 State Domestic Preparedness Support Program*, Washington, DC.

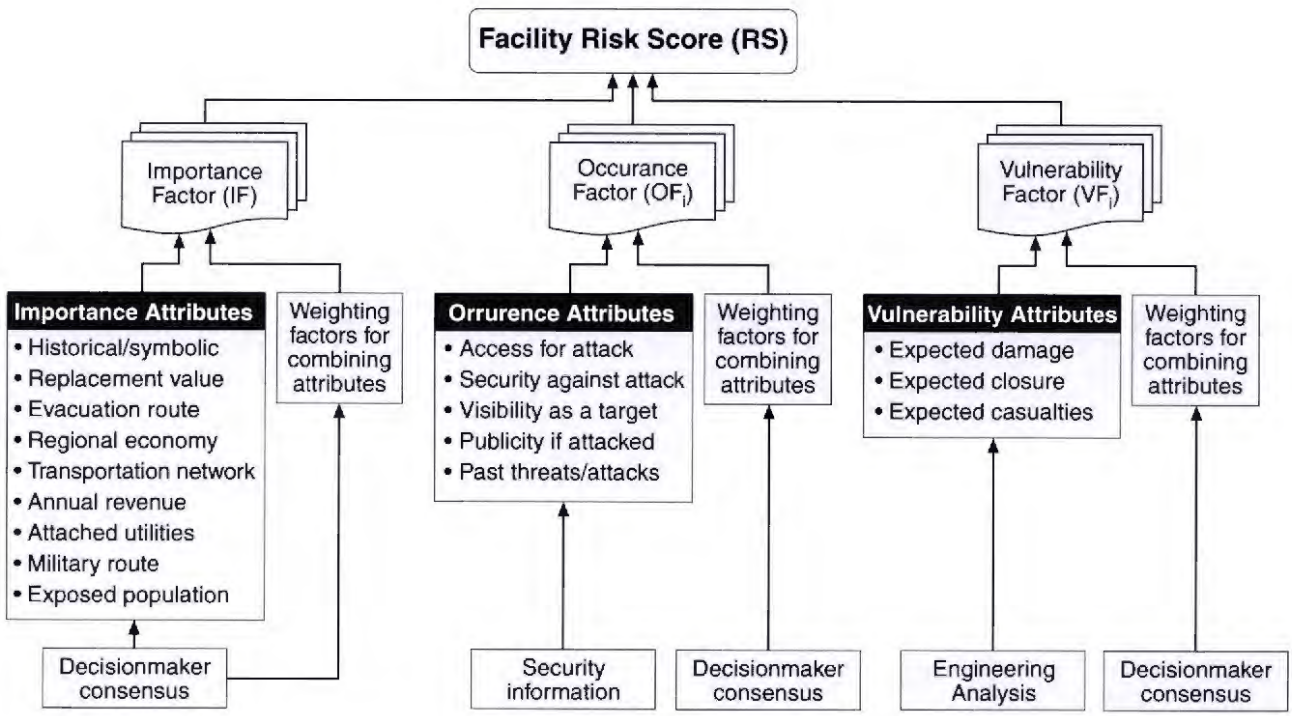


Figure C-1. Components in Risk Assessment for an Individual Facility

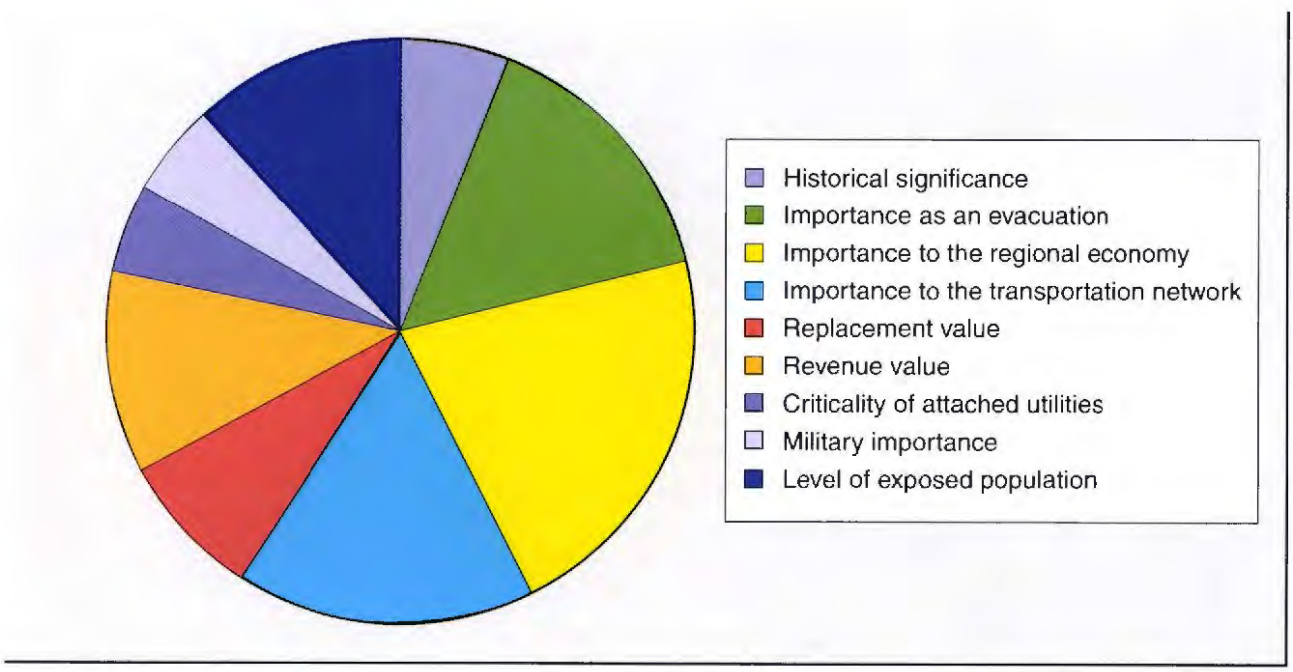


Figure C-2. Relative Weights for Attributes Used to Compute Importance Factor

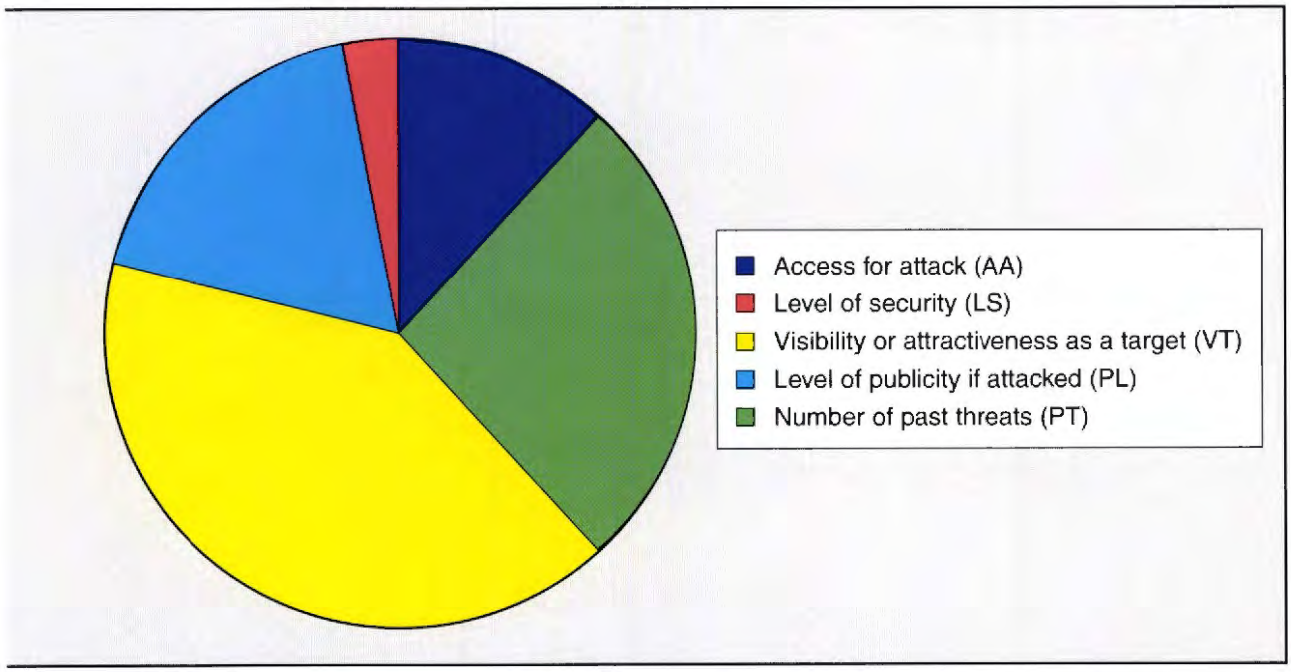


Figure C-3. Relative Weights for Attributes Used to Compute Occurrence Factor

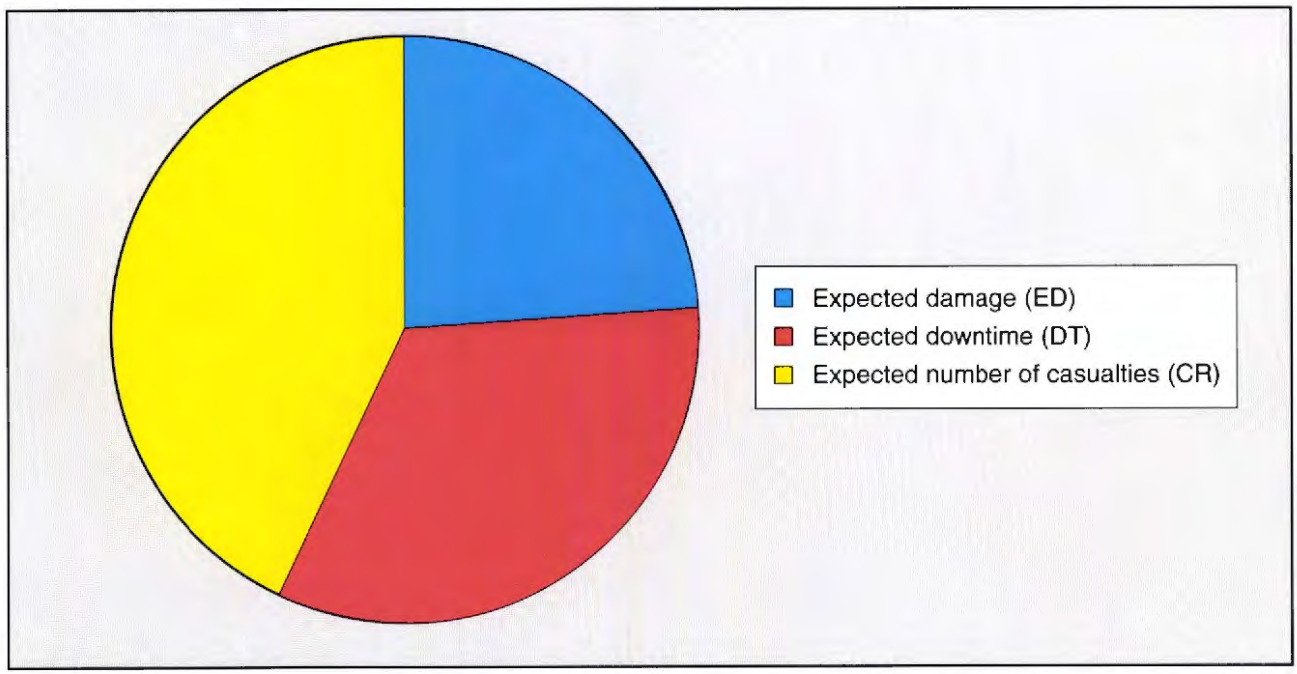


Figure C-4. Relative Weights for Attributes Used to Compute Vulnerability Factor

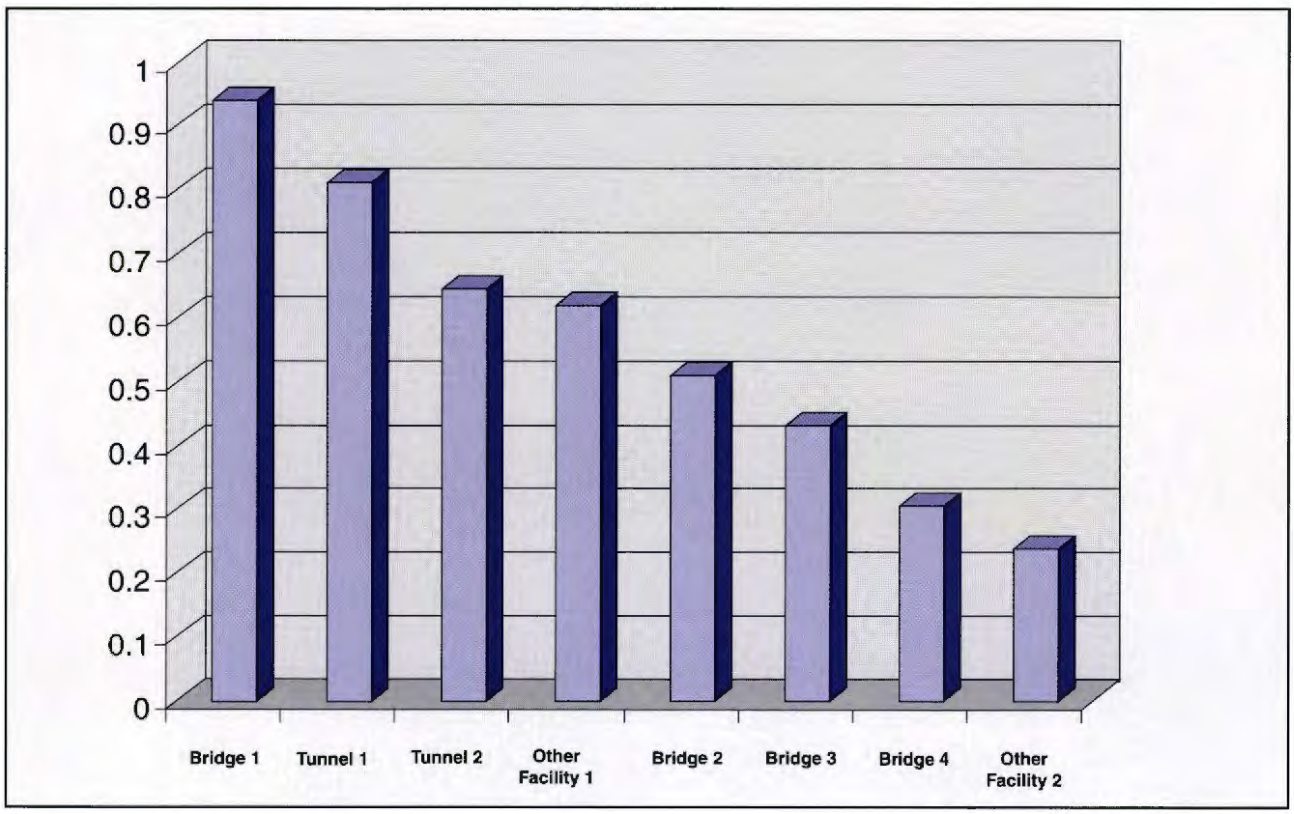


Figure C-5. Ranking of Facilities by Importance Factor

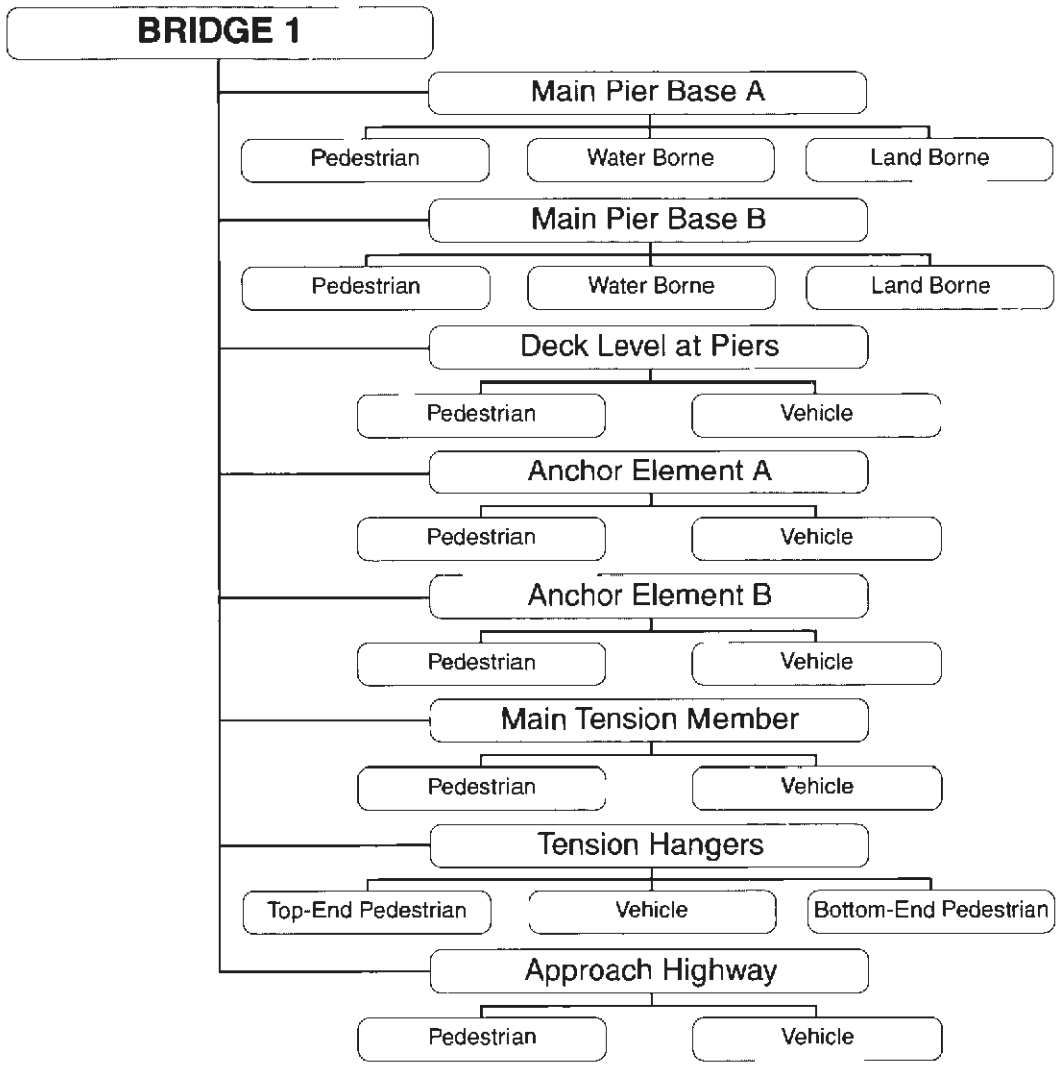


Figure C-6. Breakdown of Bridge 1 into Vulnerable Components and Mode of Access

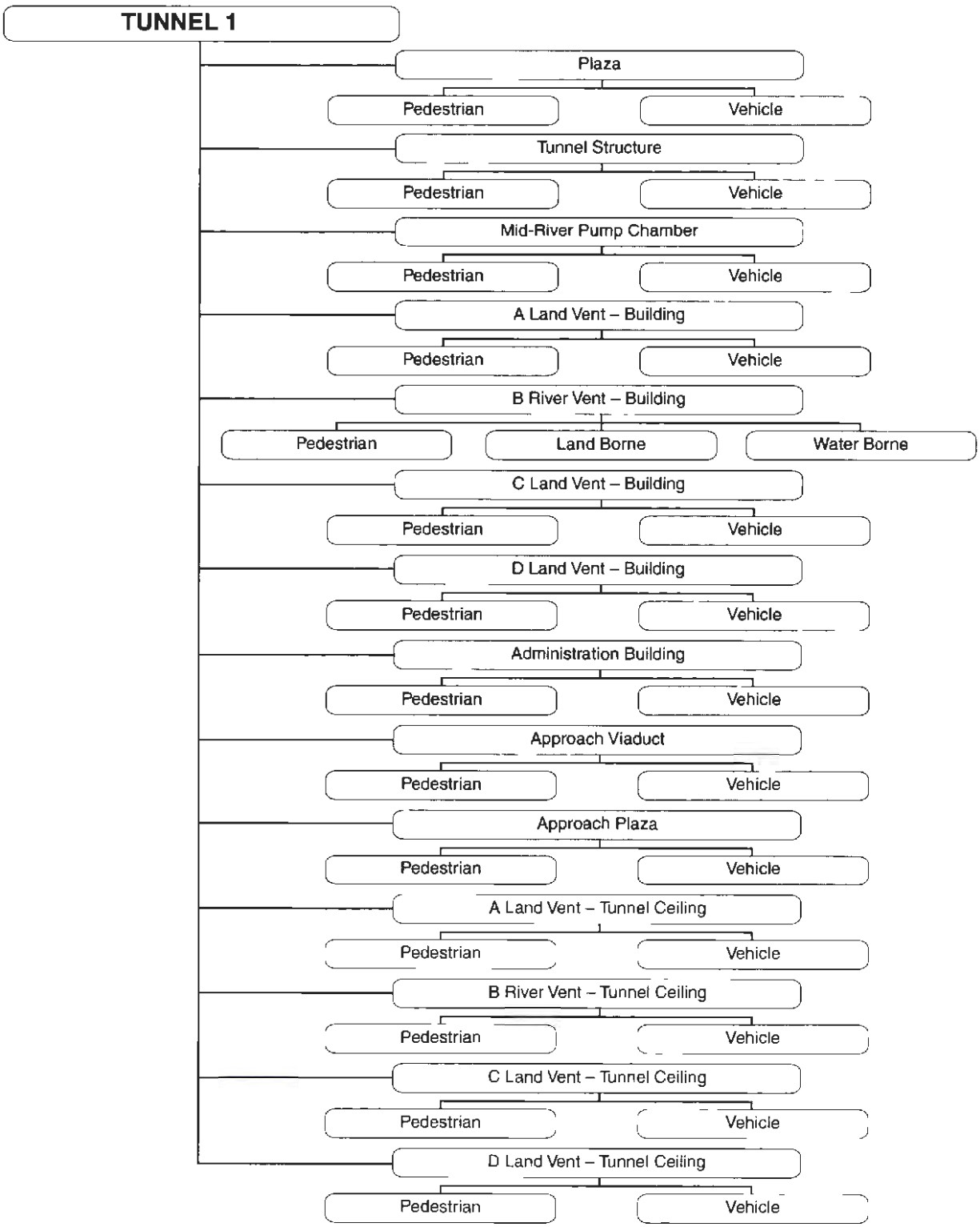


Figure C-7. Breakdown of Tunnel 1 into Vulnerable Components and Mode of Access

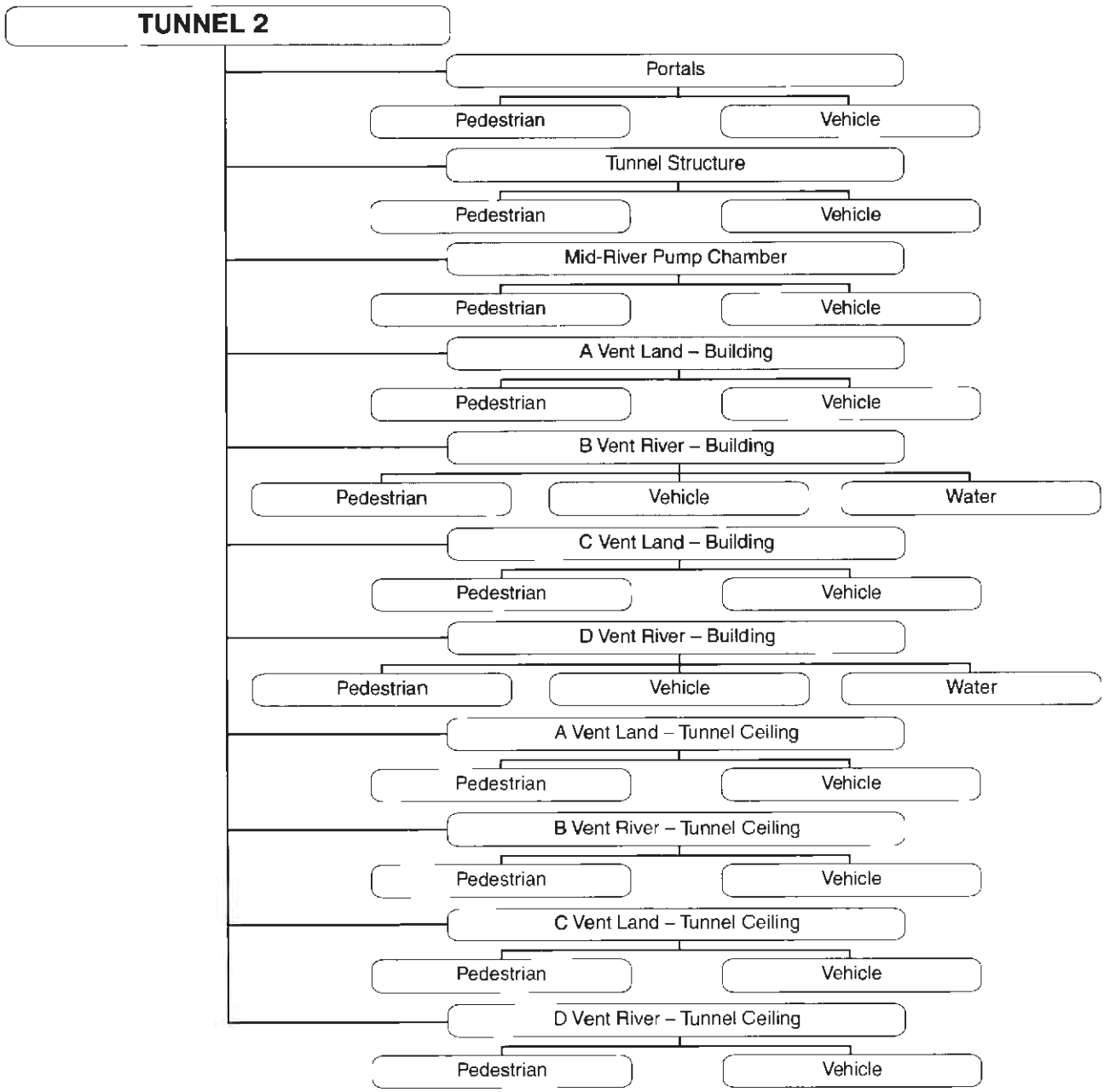


Figure C-8. Breakdown of Tunnel 2 into Vulnerable Components and Mode of Access

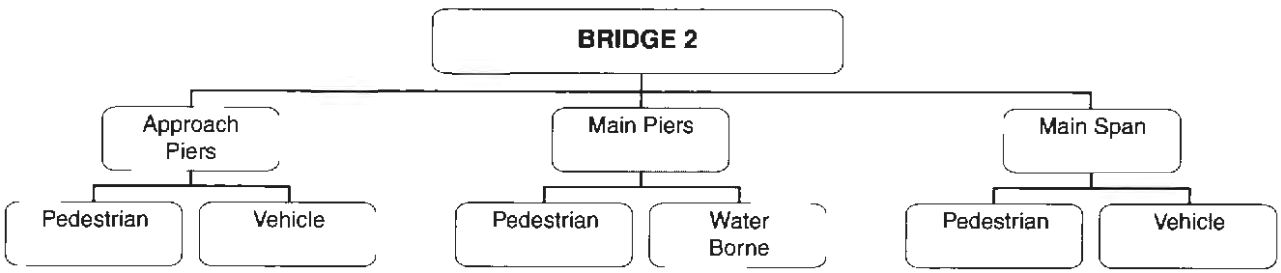


Figure C-9. Breakdown of Bridge 2 into Vulnerable Components and Mode of Access

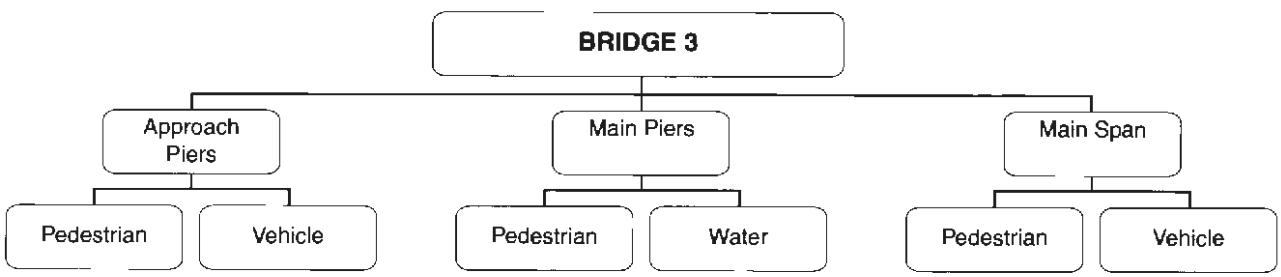


Figure C-10. Breakdown of Bridge 3 into Vulnerable Components and Mode of Access

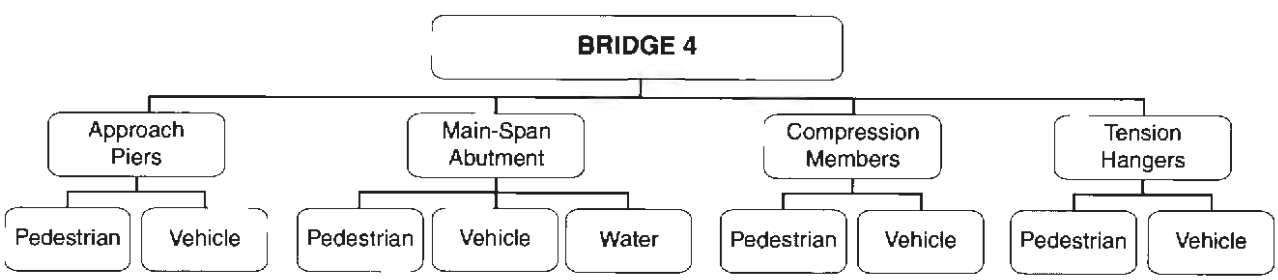


Figure C-11. Breakdown of Bridge 4 into Vulnerable Components and Mode of Access

Rank	Facility	Location	Reduction in Risk Score	Project Cost (x$1,000)
1	Bridge 1	Main Pier Base B	0.16	753
2	Other Facility 1	Element A	0.30	1,872
3	Tunnel 1	Vent Buildings – Buildings	0.48	7,857
4	Other Facility 1	Element B	0.34	8,243
5	Bridge 1	Anchor Element B	0.11	2,840
6	Bridge 1	Anchor Element A	0.10	2,840
7	Other Facility 1	Element C	0.23	6,982
8	Tunnel 1	Approach Viaduct	0.12	3,891
9	Bridge 1	Main Pier Base A	0.32	13,937
10	Bridge 4	Tension Hangers	0.05	2,944
11	Tunnel 1	Vent Buildings – Tunnel Ceilings	0.16	12,619
12	Tunnel 1	Approach Plaza	0.03	2,787
13	Tunnel 2	Vent Buildings – Buildings	0.10	9,142
14	Tunnel 2	Vent Buildings – Tunnel Ceilings	0.13	12,523
15	Bridge 1	Deck Level	0.30	30,869
16	Bridge 2	Main Piers	0.10	12,048
17	Other Facility 1	Element D	0.05	7,432
18	Tunnel 1	Administration Building	0.01	434
19	Bridge 1	Tension Hangers	0.07	12,363
20	Bridge 1	Approach Highway	0.15	32,686
21	Other Facility 2	Element A	0.01	1,950
22	Bridge 4	Main-Span Abutment	0.02	5,891
23	Bridge 3	Main Piers	0.09	24,649
24	Other Facility 1	Element E	0.10	31,754
25	Other Facility 2	Element B	0.02	6,896
26	Tunnel 1	Tunnel Structure	0.51	222,723
27	Tunnel 2	Tunnel Structure	0.35	186,735
28	Other Facility 1	Element F	0.03	20,516
29	Bridge 4	Compression Members	0.01	8,687
30	Bridge 2	Main Span	0.08	64,996
31	Bridge 3	Main Span	0.07	108,718
32	Tunnel 1	Portals	0.01	16,040
33	Tunnel 2	Portals	0.01	14,287

Table C-1. Final Ranking of Mitigation Projects by Benefit/Cost Ratio

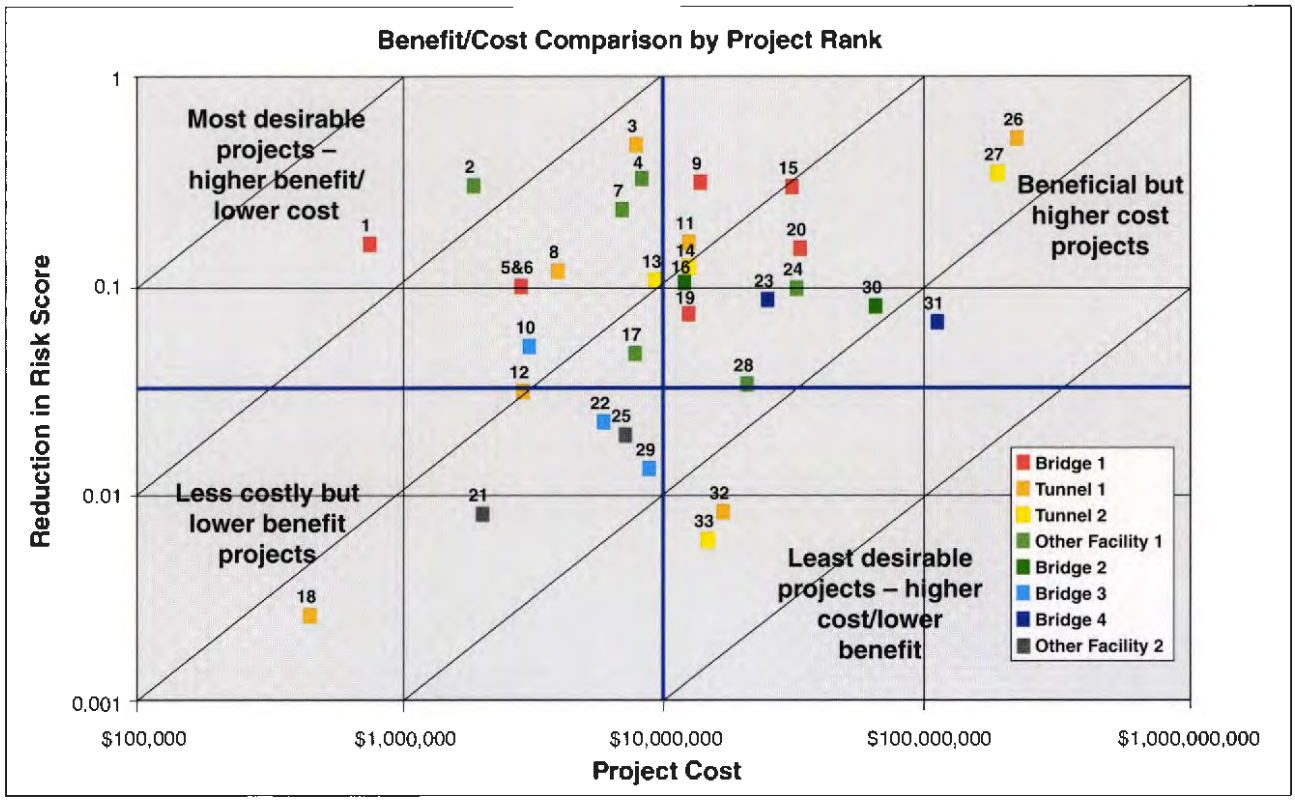
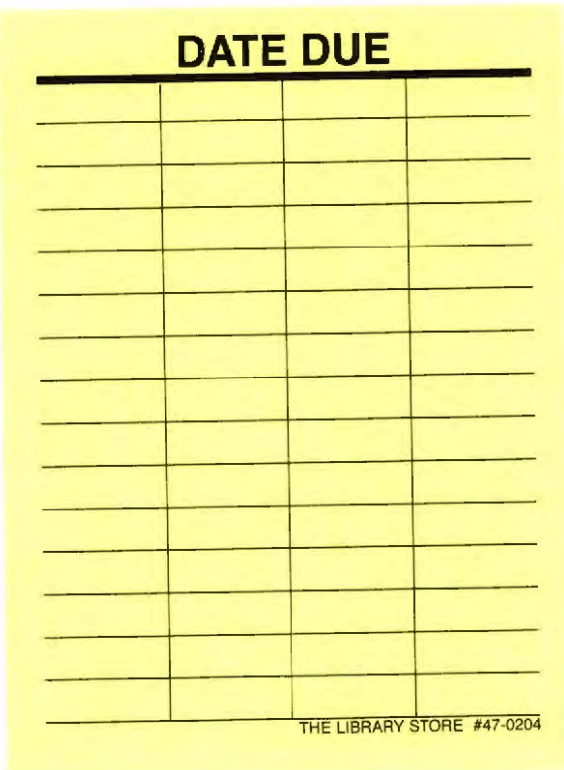


Figure C-12. Chart Illustrating Comparison of Benefits and Costs for All Mitigation Projects



FHWA-IF-03-036
HIBT/10-03 (3M)E