BLUE RIBBON PANEL RECOMMENDATIONS FOR BRIDGE AND TUNNEL SECURITY

James D. Cooper[1], Michael C. Smith[2], and Steven L. Ernst[3]

Abstract

The September 11, 2001 attacks on the World Trade Center and the Pentagon issued in a new era of challenges for infrastructure owners and bridge and highway engineers not only in the United States, but also around the world. Although the September 11th attacks targeted buildings, threats against bridges and tunnels and other highway infrastructure in various parts of the U. S. and undoubtedly elsewhere 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.

This paper, taken from a report (1) by a special Blue Ribbon Panel (BRP) that was appointed by the Federal Highway Administrator at the request of the American Association of State and Highway Transportation Officials (AASHTO) summarizes their work to 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 and operators. A PDF version of the Panel's full report is available on the Federal Highway Administration (FHWA) website at:
http://www.fhwa.dot.gov/bridge/security/brpcover.htm

I. Introduction

A Blue Ribbon Panel (BRP) of bridge and tunnel experts from professional practice, academic, 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 success and safety of the transportation system, combined with the perceived existing 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 Blue Ribbon Panel 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, which 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. Among the approximately

[1]P.E., Bridge Technology Consultant, Purcellville, VA.

[2]Ph.D., Senior Scientist/Ass't Vice President, Science Applications International Corporation, Charlottesville, VA.

[3]P.E., Structural Engineer, Federal Highway Administration, Washington, D.C.

600,000 bridges in the United States, preliminary studies indicate that there are approximately 1000 where substantial casualties, economic disruption and other societal ramifications would result from isolated attacks. *The system has vulnerabilities, which must be addressed. This is important enough to be a matter of national security policy for the United States.*

With prospects of losses and related significant 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 the nations' well being. Typically, bridge owners manage risks associated with natural hazards using well developed risk assessment methods based on mature occurrence models that allow them to make informed trade-off decisions among mitigation alternatives. Unlike the case of natural hazards, owners are in the dawn of an era in which they feel overwhelmed by uncertainties about the occurrence and potential costs of terrorist attacks and about their legal responsibilities to protect the users of their structures. 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.

The Blue Ribbon Panel made seven overarching recommendations to accomplish the overall goal of reducing the vulnerability of bridges and tunnels to terrorist attacks that fall into three areas related to institutional, technical, and fiscal responsibilities. The recommendations included the need for interagency coordination including the development of outreach and communication strategies, new funding sources for bridge and tunnel security and technical recommendations.

This paper focuses on the Panel's strategy and recommendations for planning, design and engineering approaches to improve bridge and tunnel security. Included are suggested countermeasure options and operational security practices.

II. Panel Strategy for Developing Bridge and Tunnel Security

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
Foundations for Policy	• Criteria establishing Investment Priorities
Planning, Design, and Engineering	• Institutional Continuity • Design Review for Secure Structures • Research and Development Needed to Support "Design for Security • Design Criteria • Design Specifications
Management and Operational Practices	•Best Practices •Practice Review • Institutional Relationships • Preparedness • Personnel and Vehicle Security • Communications/Outreach
Information Security	• Procurement Practices • Information Security
Mobilization ("Notice") and Response ("Trans-event")	• Threat Warning • Early Response • Initial Response
Recovery ("Post-event")	• Damage Assessment • Functional Continuity

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

III. Overarching Panel Recommendations For Planning, Research and Development, and Design and Engineering

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 (2). 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 (3). However, these protection challenges can be mitigated through technical collaboration and coordination.

Planning

A planning or review and prioritization 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), (2). 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 (4).

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 (5). 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
- 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
- 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:

$$\mathbf{R = O \times V \times I}$$

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.

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 anyone 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).

The panel made near-term (3-6 months), mid-term (6-12 months) and long-term (12-18 month) recommendations for 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 (6).

Research and Development

The Panel supported the need for a strong Research and Development program to advance design practice and engineering. Areas in need of R&D are described next. 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	Multi-girder/Freeway Overpass Bridges
• Suspender ropes, stay cables • Tower leg • Main cable • Orthotropic steel deck • Reinforced and pre-stressed 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	• Decks • Connections • Piers

The goal of the R&D initiatives recommended by the Panel 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 the FHWA, AASHTO, and other government-sponsored research organizations, including universities and federal laboratories. Additionally, these five recommendations are interrelated and interdependent and should be pursued simultaneously. They include:

(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:

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

Long-term:

- 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:

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

Long-term:

- Determine progressive collapse potential of various bridge and tunnel systems

(5) Develop mitigation measures and hardening technologies

Short-term:

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

Long-term:

- 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.

Design and Engineering

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:

(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.
    (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 be 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.

The Panel recommends that the 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

described in the next section. Countermeasures should be ranked and implemented based on a technically sound cost-benefit analysis such as described in the full report.

IV. Countermeasure Options (7)

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
- 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 "blowout" 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

V. 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)

VI. Summary

Terrorism against American citizens and assets is real and growing. 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. There is no question that terrorists are interested in bridges and tunnels as attractive targets of opportunity to disrupt societal function.

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 and the American Association of State Highway and Transportation Officials acknowledges that the nation's bridges and tunnels are vulnerable to terrorist attacks. The intent of this paper was to summarize BRP recommended policies and actions to reduce the probability of catastrophic structural damage that could result in substantial human casualties, economic losses, and socio-political damage.

Appendix

Blue Ribbon Panel Members

- 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
- 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

References

(1) Recommendations For Bridge and Tunnel Security, Blue Ribbon Panel on Bridge and Tunnel Security, Washington D.C., September 2003. (Also, FHWA Website at: http://www.fhwa.dot.gov/bridge/security/brpcover.htm

(2) A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection, prepared for AASHTO by Science Applications International Corporation, Vienna, VA, under NCHRP Project 20-7/Task 151B, SAIC, May, 2002.

(3) 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.

(4) Briefing to the FHWA/AASHTO Blue Ribbon Panel on Bridge and Tunnel Security, Tom Reilly, Transportation Security Administration, Department of Homeland Security, March 27, 2003.

(5) Briefing, "Transportation Security Update," Tom Rummel, P.E., Project Development Section, Bridge Division, Texas Department of Transportation, February 2003.

(6) 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 under NCHRP Project 20-59/Task 5, October 2002.

(7) Design of Bridges for Security, presentation by Capt. David Winget, University of Texas Department of Civil Engineering at NCHRP Bridge Infrastructure Vulnerability Assessment Workshop, February 10, 2003.

Acknowledgement

The authors are indebted to the Blue Ribbon Panel Members, a group of 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. The panel's initiative and collective wisdom reflected in their report will help America and perhaps other countries meet future challenges to strengthen the transportation infrastructure network.

The authors also acknowledge the contributions of numerous others whose contributions throughout Blue Ribbon Panel deliberations formed the basis for portions of the full report. Specific recognition is given to: Mr. Dan Hartman, Transportation Security Administration, Department of Homeland Security; Dr. Anthony Kane, Director of Engineering, American Association of State and Highway Transportation Officials (AASHTO); Mr. Richard Land, State Bridge Engineer, California DOT (CALTRANS); Mr. Paul Liles, State Bridge Engineer, Georgia DOT; Mr. Stephan Parker, Senior Program Manager, National Cooperative Highway Research Program; Ms. Mary Lou Ralls, State Bridge Engineer, Texas DOT; Mr. James Ray, Research Engineer, ERDC, Corps of Engineers; Mr. Tom Reilly, Transportation Security Administration, Department of Homeland Security; and Capt. David Winget, Graduate Student, University of Texas, Austin.