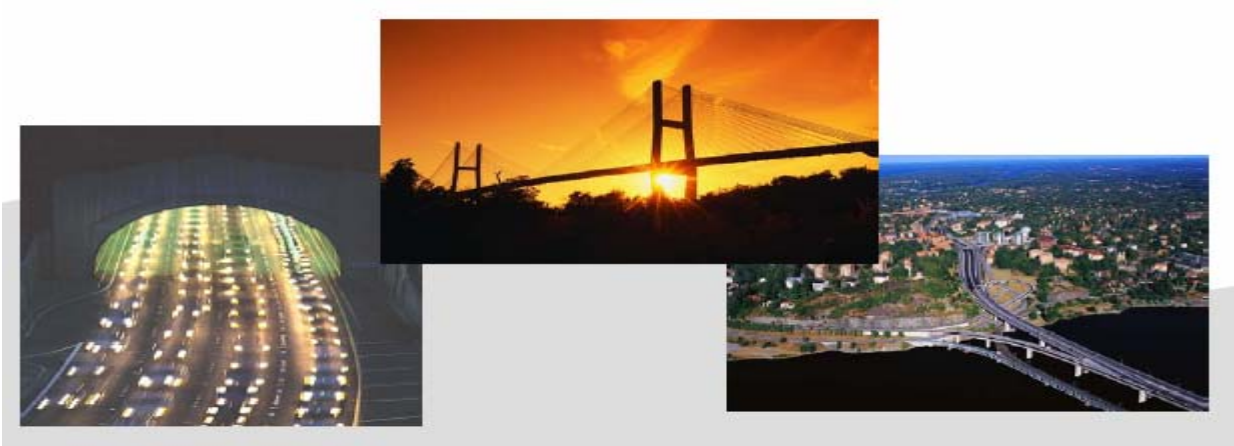
23E CONGRÈS MONDIAL DE LA ROUTE PARIS 2007

23rd WORLD ROAD CONGRESS PARIS 2007

Highway Systems Security
PIARC TC 3.2
Workgroup 3

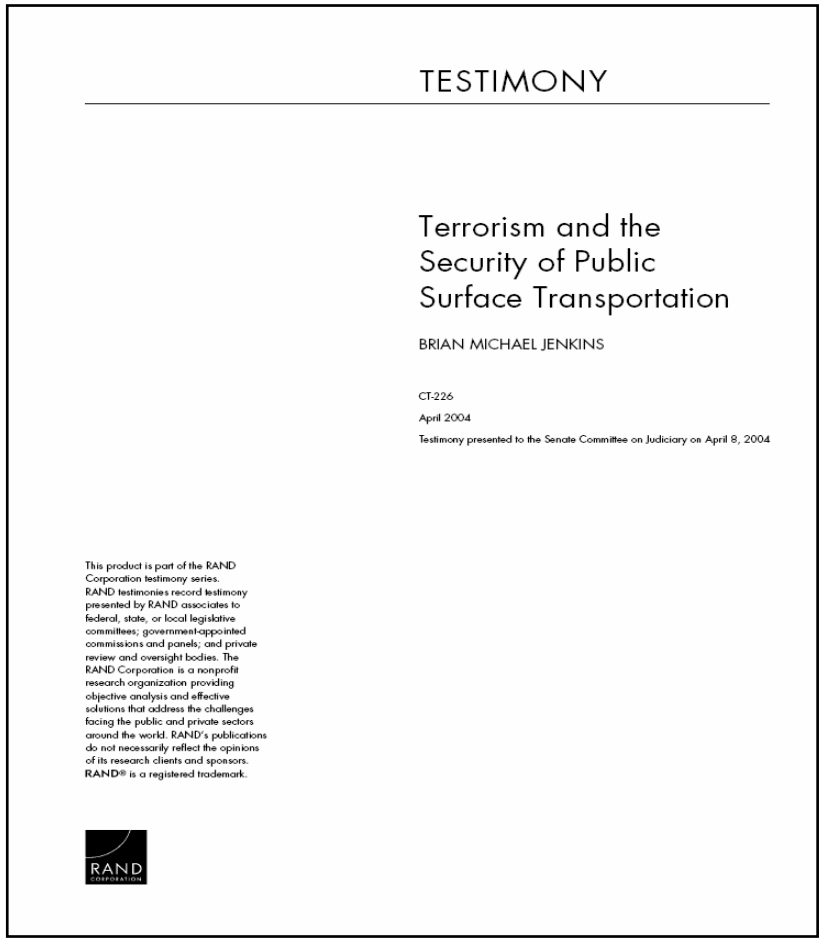


Michel Cloutier

- Transport Canada
- Director, CANUTEC
- Transportation of Dangerous Goods

Highway Systems - A Target For Terrorism

- **Public Transportation**
  - Automobiles
  - Trucks
  - Buses
  - Trains
  - Subways
  - Aviation
  - Ships, etc.
- **Infrastructures**
  - Highways and Roads
  - Bridges
  - Tunnels
  - etc…



TESTIMONY

Terrorism and the Security of Public Surface Transportation

BRIAN MICHAEL JENKINS

CT-226

April 2004

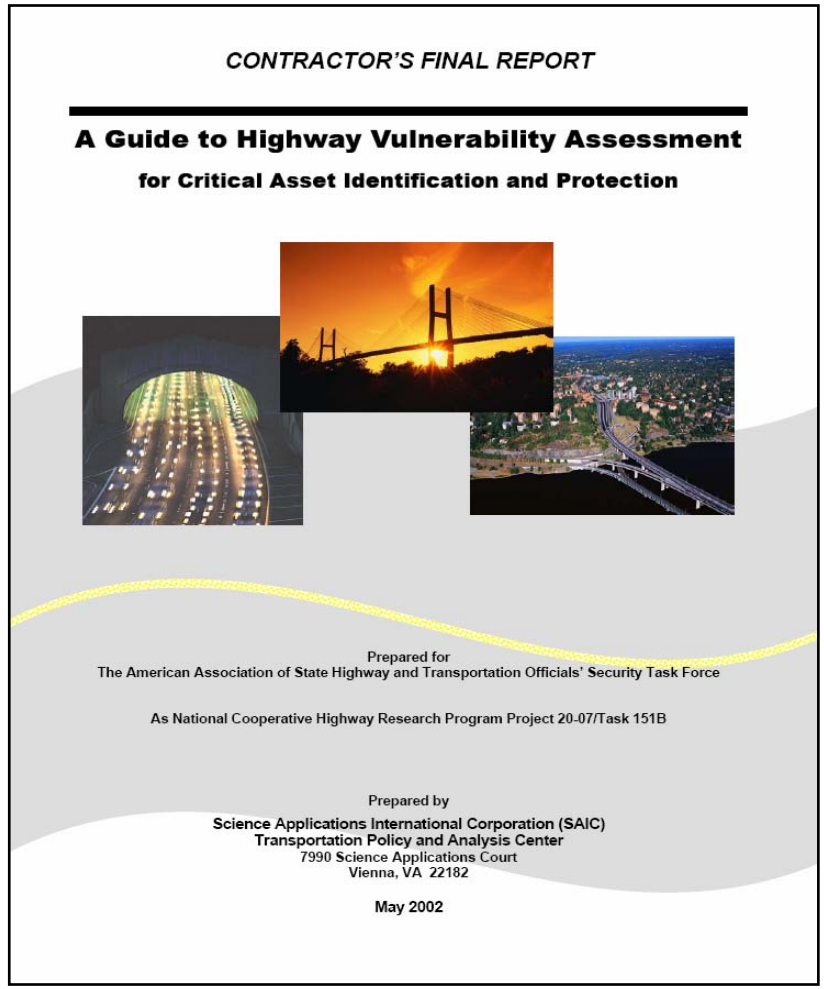
Testimony presented to the Senate Committee on Judiciary on April 8, 2004

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

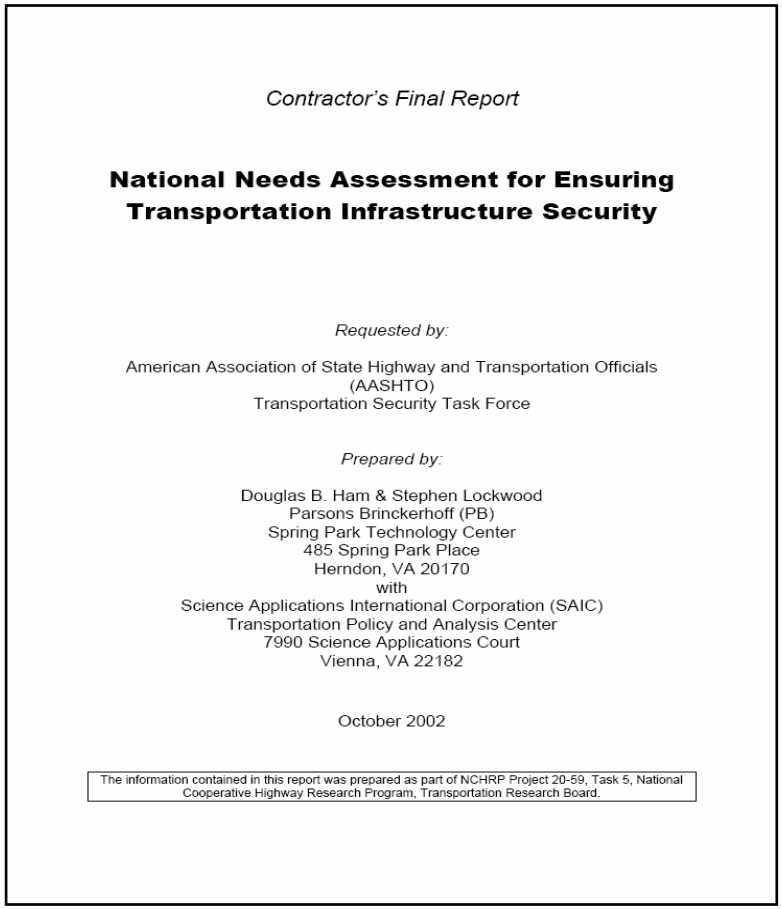
RAND CORPORATION

Task Force Report Summary

- **Assess the vulnerabilities of physical assets such as bridges, tunnels, roadways, and inspection and traffic operation facilities, among others**
- **Develop possible countermeasures to deter, detect, and delay the impact of threats to such assets**



Task Force Report Summary (con't)



Contractor's Final Report

National Needs Assessment for Ensuring Transportation Infrastructure Security

Requested by:

American Association of State Highway and Transportation Officials
(AASHTO)
Transportation Security Task Force

Prepared by:

Douglas B. Ham & Stephen Lockwood
Parsons Brinckerhoff (PB)
Spring Park Technology Center
485 Spring Park Place
Herndon, VA 20170
with
Science Applications International Corporation (SAIC)
Transportation Policy and Analysis Center
7990 Science Applications Court
Vienna, VA 22182

October 2002

The information contained in this report was prepared as part of NCHRP Project 20-59, Task 5, National Cooperative Highway Research Program, Transportation Research Board.

- **Estimate the capital and operating costs of such countermeasures, and**
- **Improve security operational planning for better protection against future acts of terrorism (emergency plans)**

Vulnerability Assessment Phases

A typical schedule for conducting all three phases of the vulnerability assessment is shown in Figure 3.

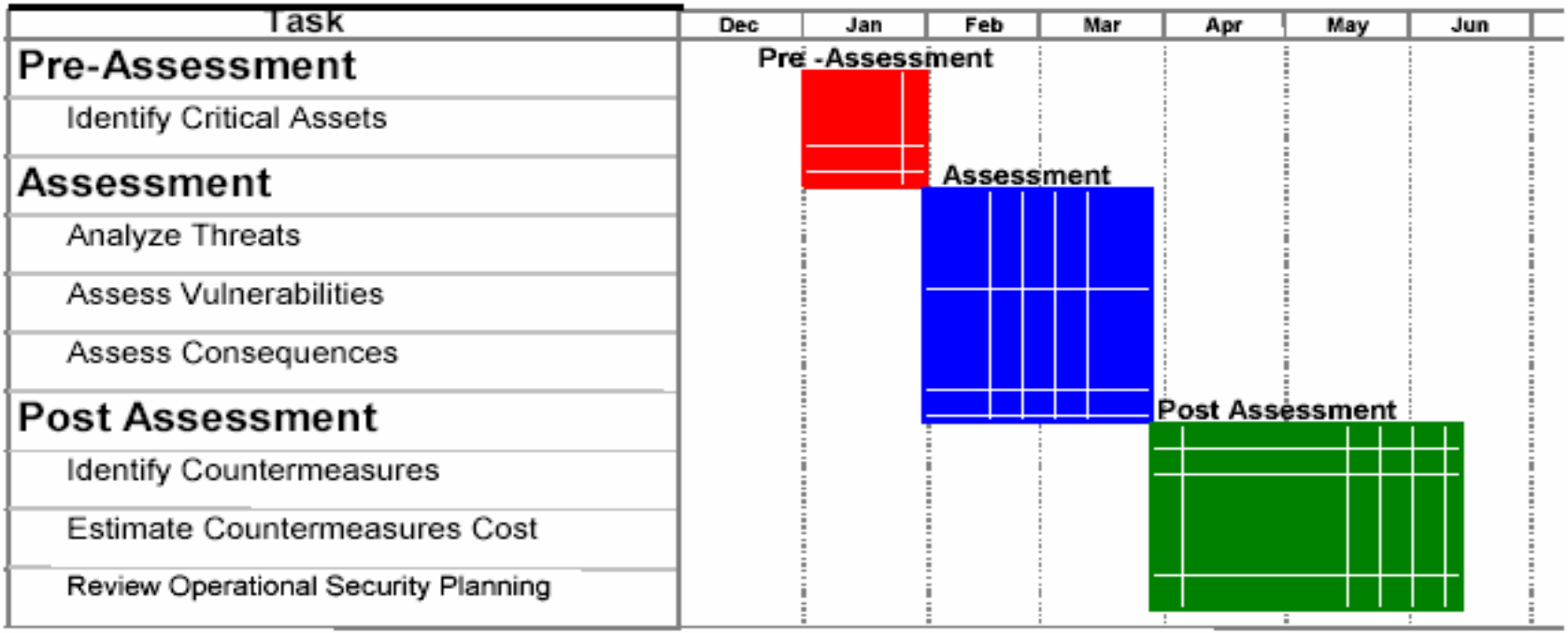


Figure 3 – Typical Vulnerability Assessment Schedule

Vulnerability Assessment Overview

General Approach

- **Step 1: Identify Critical Assets**
- **Step 2: Assess Vulnerabilities**
- **Step 3: Assess Consequences**
- **Step 4: Identify Countermeasures**
- **Step 5: Estimate Countermeasures Cost**
- **Step 6: Implement and review emergency plans**

Step 1: Identify Critical Assets

Table 1 - Critical Transportation Assets

INFRASTRUCTURE	*FACILITIES*	*EQUIPMENT*	*PERSONNEL*
▪ Arterial Roads ▪ Interstate Roads ▪ Bridges ▪ Overpasses ▪ Barriers ▪ Roads Upon Dams ▪ Tunnels	▪ Chemical Storage Areas ▪ Fueling Stations ▪ Headquarters Buildings ▪ Maintenance Stations/Yards ▪ Material Testing Labs ▪ Ports of Entry ▪ District/Regional Complexes ▪ Rest Areas ▪ Storm Water Pump Stations ▪ Toll Booths ▪ Traffic Operations Centers ▪ Vehicle Inspection Stations ▪ Weigh Stations	▪ Hazardous Materials ▪ Roadway Monitoring ▪ Signal & Control Systems ▪ Variable Messaging System ▪ Vehicles ▪ Communications Systems	▪ Contractors ▪ Employees ▪ Vendors ▪ Visitors

Although using all four categories is recommended, any one of these categories can be eliminated if it is not considered critical to the department's mission.

Step 1: Identify Critical Assets

Table 2 - Critical Asset Factors and Values

CRITICAL ASSET FACTOR	VALUE	DESCRIPTION
Deter/Defend Factors		
A) Ability to Provide Protection	1	Does the asset lack a system of measures for protection? (i.e., Physical or response force)
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (i.e., Due to location, prominence, or other factors)
Loss and Damage Consequences		
C) Casualty Risk	5	Is there a possibility of serious injury or loss of life resulting from an attack on the asset?
D) Environmental Impact	1	Will an attack on the asset have an ecological impact of altering the environment?
E) Replacement Cost	3	Will significant replacement cost (the current cost of replacing the asset with a new one of equal effectiveness) be incurred if the asset is attacked?
F) Replacement/Down Time	3	Will an attack on the asset cause significant replacement/down time?
Consequences to Public Services		
G) Emergency Response Function	5	Does the asset serve an emergency response function and will the action or activity of emergency response be affected?
H) Government Continuity	5	Is the asset necessary to maintain government continuity?
I) Military Importance	5	Is the asset important to military functions?
Consequences to the General Public		
J) Available Alternate	4	Is this the only asset that can perform its primary function? (i.e., There are no alternate facilities that will substitute adequately if this asset is damaged or destroyed)
K) Communication Dependency	1	Is communication dependent upon the asset?
L) Economic Impact	5	Will damage to the asset have an effect on the means of living, or the resources and wealth of a region or state?
M) Functional Importance	2	Is there an overall value of the asset performing or staying operational?
N) Symbolic Importance	1	Does the asset have symbolic importance?

Step 1: Critical Asset Factor Scoring

Table 3 - Critical Asset Scoring

CRITICAL ASSET	CRITICAL ASSET FACTOR													TOTAL SCORE (x)
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Asset 1															
Asset 2															
Asset 3															
Asset 4															
Asset 5															
Asset n															

The total score calculated in this step (x) will be used in calculating the criticality coordinate of each asset (X) in Step 3, as follows:

Criticality Coordinate (X) = $(x/ C_{max})*100$

Step 2: Assess Vulnerabilities

Table 7 – Vulnerability Factor Default Values and Definitions

VULNERABILITY FACTOR and DEFAULT VALUE			*DEFINITION*
Visibility and Attendance	LEVEL OF RECOGNITION (A)	1	Largely invisible in the community
		2	Visible by the community
		3	Visible Statewide
		4	Visible Nationwide
		5	Visible Worldwide
	ATTENDANCE/ USERS (B)	1	Less than 10
		2	10 to 100 (Major Incident per FEMA)
		3	100 to 1000
		4	1000 to 3000
		5	Greater than 3000 (Catastrophic Incident per FEMA)
Access to the Asset	ACCESS PROXIMITY (C)	1	Asset with no vehicle traffic and no parking within 50 feet
		2	Asset with no unauthorized vehicle traffic and no parking within 50 feet
		3	Asset with vehicle traffic but no vehicle parking within 50 feet
		4	Asset with vehicle traffic but no unauthorized vehicle parking within 50 feet
		5	Asset with open access for vehicle traffic and parking within 50 feet
	SECURITY LEVEL (D)	1	Controlled and protected security access with a response force available
		2	Controlled and protected security access without a response force
		3	Controlled security access but not protected
		4	Protected but not controlled security access
		5	Unprotected and uncontrolled security access
Site Specific Hazards	RECEPTOR IMPACTS (E)	1	No environmental or human receptor effects
		2	Acute or chronic toxic effects to environmental receptor(s)
		3	Acute and chronic effects to environmental receptor(s)
		4	Acute or chronic effects to human receptor(s)
		5	Acute and chronic effects to environmental and human receptor(s)
	VOLUME (F)	1	No materials present
		2	Small quantities of a single material present
		3	Small quantities of multiple materials present
		4	Large quantities of a single material present
		5	Large quantities of multiple materials present

Step 2: Vulnerability Factor Scoring

Vulnerability Factor (y) = (A * B) + (C * D) + (E * F)

According to Table 7, for any critical asset, the lowest attainable vulnerability factor score is 3 and the highest attainable score is 75.

The vulnerability factor (y) will be used to calculate the vulnerability coordinate (Y) in the next step, as follows:

Vulnerability Coordinate (Y) = (y/75)* 100

Table 8 - Vulnerability Factor Scoring

CRITICAL ASSET	VULNERABILITY FACTOR											TOTAL SCORE (y)
	(A	*	B)	+	(C	*	D)	+	(E	*	F)	
	1-5	*	1-5	+	1-5	*	1-5	+	1-5	*	1-5	
Asset 1												
Asset 2												
Asset 3												
Asset 4												
Asset 5												
Asset n												

Step 3: Assess Consequences

Figure 5 - Criticality and Vulnerability Matrix

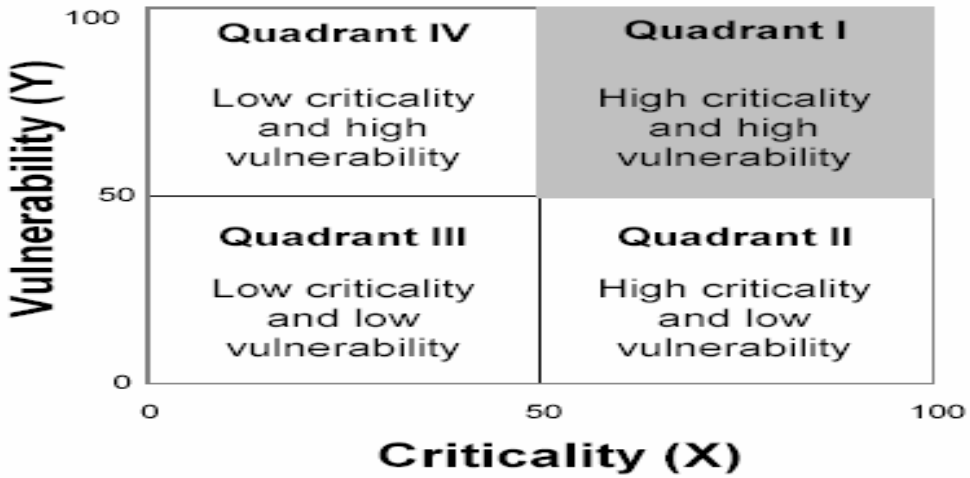


Figure 5 helps prioritize critical assets by the greatest level of consequence based on the critical asset factors and vulnerabilities evaluated previously. Quadrant I identifies the assets with the highest criticality and vulnerability for implementing countermeasures.

Illustrative Example

Using the Smith Bridge as an example, the X and Y coordinates for this critical asset were calculated as follows:

$$X = (43/43) * 100 = 100$$

$$Y = (43/75) * 100 = 57$$

These coordinates (100, 57) place the Smith Bridge in Quadrant I. The coordinates and related quadrants for the other critical assets were calculated in the same manner and are identified in Table 10.

Blue Ribbon Panel Document

Risk Assessment Method

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

- R is the Risk factor
- O is the Occurrence factor
- V is the Vulnerability factor
- I is the Importance factor

- The equation reflects an approach similar to that for assessing seismic and other natural hazards.

Blue Ribbon Panel Document

Risk Assessment Method

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

- O value reflects likelihood the bridge /tunnel (or component) will be attacked
- Occurrence attributes are: Attractiveness as a target, Security level against attack, Visibility as a target, Publicity if attacked, Prior threats/attacks
- Input to value comes from law enforcement and security experts

Blue Ribbon Panel Document

Risk Assessment Method

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

- V value reflects the likely degree of damage to the bridge/tunnel (or component) from an attack (threat)
- Vulnerability attributes are: expected damage, expected downtime, expected number of casualties
- Input to value comes from engineering analysis and expertise

Blue Ribbon Panel Document

Risk Assessment Method

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

- I value is a characteristic of the bridge /tunnel facility that reflects the consequence of its loss, independent of the type of hazard that might damage it
- Importance attributes: historical value, evacuation route, regional economy, cost/time to replace, revenue loss, critical utilities, exposed population, military value
- Input to value comes from owners, operators, users, regional government

Step 4: Identify Countermeasures

Deter attacks by the possibility of exposure, capture, or failure due to visible countermeasures

- **Detect potential attacks before they occur and provide the appropriate response force**

- **Defend the asset by delaying and distancing the attacker from the asset and protecting the asset from the effects of weapons**

Step 4: Identify Countermeasures (con't)

- **DESIGN - Blue Ribbon Panel, "Recommendations for Bridge and Tunnel Security" recommends that Research and Development (R&D) is Needed to Support "Design for Security"**
- **DESIGN/REDESIGN – "National Needs Assessment for Ensuring Transportation Infrastructure Security" discusses the design/redesign of the asset to minimize the potential effects of WMD and conventional explosives**
- **The redesign aspect covers retrofit costs to both bridge and tunnels in the United States as an example**

Step 4: Identify Countermeasures (con't)

Examples of Countermeasures for Bridges

Example: Maryland's Countermeasures

Maryland has devised a list of post September 11 countermeasure initiatives for each of its high priority transportation facilities. These initiatives include:

- Built-in monitors on bridges
- Motion detection devices below bridges
- Increased armed security
- Regular checking of truck traffic
- Application of X-ray technology
- Improved training for toll collectors and other tunnel personnel
- Enforcement of HAZMAT requirements
- Increased lighting
- CCTV cameras for surveillance
- No-fly zones around bridges
- Suspension cable protection
- Patrol boats under and around bridges

Example: Texas's Potential Countermeasures for Bridges

Texas identified the following on their list of countermeasures for critical bridges:

- Eliminate parking areas beneath bridge
- Restrict ingress and egress routes from adjacent areas
- Provide additional lighting
- Limit/monitor access to plans of existing bridges
- Install motion sensors or other active sensors
- Install surveillance cameras
- Apprise local law enforcement officials of critical bridges
- Provide column protection
- Provide pass-through in concrete median barriers
- Install advance warning system

Step 4: Identify Countermeasures (con't)

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

Step 5: Estimate Countermeasures Cost

Objective: estimate the capital and operating costs for implementing the selected countermeasures

COUNTERMEASURE DESCRIPTION	COUNTER-MEASURE FUNCTION			ESTIMATED RELATIVE COST (H/M/L)		
	Deter	Detect	Defend	Capital	Operating	Maintenance
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity.	✓			L	M	L
Institute full-time surveillance at the most critical assets where alternate routes are limited or have not been identified.	✓	✓		H	H	H
Eliminate parking under the most critical bridges. Elimination of the parking can be accomplished with concrete barriers.	✓			L	L	L
Place barriers in such a way as to eliminate ease of access where a vehicle could be driven right up to the asset.	✓		✓	L	L	L
Install security systems with video capability at all DOT facilities.	✓	✓		H	M	L
Protect ventilation intakes with barriers.	✓		✓	L	L	L
Install and protect ventilation emergency shut off systems.			✓	L	L	L
Install Mylar sheeting on inside of windows to protect employees from flying glass in the case of an explosion.	✓		✓	M	L	L
Place a full-time security officer in a guard shack to control access.	✓	✓	✓	M	M	L
Lock all access gates and install remote controlled gates where necessary.	✓		✓	H	M	M
Develop and implement a department-wide security policy.	✓			L	L	L
Limit access to all buildings through the issuance of a security badge with specific accesses identified and controlled through the card.	✓	✓		M	M	L
Train all DOT personnel to be more observant of their surroundings and potentially dangerous packages, boxes, people, etc.	✓	✓		M	M	L
Improve lighting.	✓	✓		L	L	L
Increase surveillance at tunnels by installing cameras linked to the TOC.	✓	✓		H	M	M
Add motion sensors to fences.	✓	✓		L	L	L

Step 5: Estimate Countermeasures Cost

Objective: estimate the capital and operating costs for implementing the selected countermeasures

COUNTERMEASURE DESCRIPTION	COUNTER-MEASURE FUNCTION			ESTIMATED RELATIVE COST (H/M/L)		
	Deter	Detect	Defend	Capital	Operating	Maintenance
Increase inspection efforts aimed at identifying potential explosive devices as well as increased or suspicious potential criminal activity.	✓			L	M	L
Institute full-time surveillance at the most critical assets where alternate routes are limited or have not been identified.	✓	✓		H	H	H
Eliminate parking under the most critical bridges. Elimination of the parking can be accomplished with concrete barriers.	✓			L	L	L
Place barriers in such a way as to eliminate ease of access where a vehicle could be driven right up to the asset.	✓		✓	L	L	L
Install security systems with video capability at all DOT facilities.	✓	✓		H	M	L
Protect ventilation intakes with barriers.	✓		✓	L	L	L
Install and protect ventilation emergency shut off systems.			✓	L	L	L
Install Mylar sheeting on inside of windows to protect employees from flying glass in the case of an explosion.	✓		✓	M	L	L

Step 6: Implement and review emergency plans

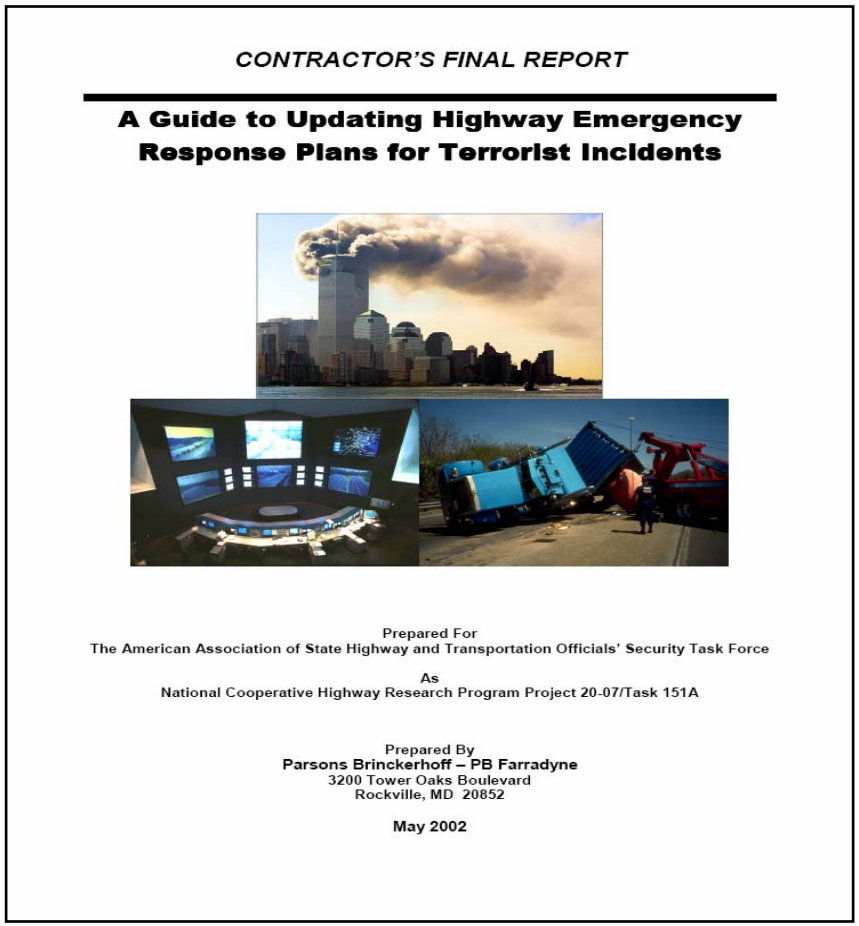
In general, emergency plans used in surface transportation provide guidance for:

- Reporting and evaluating the incident,
- Using the incident command system,
- Notifying emergency response personnel/agencies,
- Protecting personnel and equipment at the incident site

Step 6: Implement and review emergency plans (con't)

- Dispatching emergency response personnel and equipment to the site
- Evacuating passengers
- Providing briefings and information updates
- Managing the emergency
- Restoring the system to normal

Step 6: Implement and review emergency plans (con't)



CONTRACTOR'S FINAL REPORT

A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents

Prepared For
The American Association of State Highway and Transportation Officials' Security Task Force

As
National Cooperative Highway Research Program Project 20-07/Task 151A

Prepared By
Parsons Brinckerhoff – PB Farradyne
3200 Tower Oaks Boulevard
Rockville, MD 20852

May 2002

Public agencies now perceive the need for <u>updating</u> emergency response plans in light of emerging terrorist threats using weapons of mass destruction (WMD)

Step 6: Implement and review emergency plans (con't)

Differences between terrorist and non terrorist incidents:

Table 1: Similarities and Differences Between Terrorist WMD and Other Significant Emergencies

Similarities	Differences
• Mass casualties • Damage to infrastructure • With or without warning • Evacuation or displacement of citizens	• Caused by people on purpose • Will always be treated as crime scenes • May not be immediately recognizable as terrorist incidents • May not be single incidents • Place responders at higher risk due to WMD characteristics and possible planned secondary incidents • May result in widespread contamination of critical equipment and facilities • May have delayed or long-lasting effects • May expand geometrically in scope • May cause strong public reaction

Source: FEMA Web Site, Senior Officials' Workshop on Weapons of Mass Destruction

Detailed case studies

U.S. Department of Transportation

Research and Special Programs Administration

EFFECTS OF CATASTROPHIC EVENTS ON TRANSPORTATION SYSTEM MANAGEMENT AND OPERATIONS

CROSS CUTTING STUDY

U.S. Department of Transportation
John A. Volpe National
Transportation Systems Center
Cambridge, MA

January 2003

Prepared for

U.S. Department of Transportation
ITS Joint Program Office

Reference Documents

- "Effects of Catastrophic Events on Transportation System Management and Operations Cross Cutting Study", U.S. Department of Transportation, Research and Special Programs Administration, John A. Volpe National Transportation Systems Center, January 2003

- "A Guide to Updating Highway Emergency Response Plans for Terrorist Incidents", Prepared For The American Association of State Highway and Transportation Officials' Security Task Force As National Cooperative Highway Research Program Project 20-07/Task 151A Prepared By Parsons Brinckerhoff – PB Farradyne, May 2002

Reference Documents (continued)

- "A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection (Science Applications International Corporation SAIC, Transportation Policy and Analysis Center, May 2002)) Prepared for The American Association of State Highway and Transportation Officials' Security Task Force As National Cooperative Highway Research Program Project 20-07/Task 151BA
- "National Needs Assessment for Ensuring Transportation Infrastructure Security" Requested by: American Association of State Highway and Transportation Officials (AASHTO) Transportation Security Task Force Prepared by: Douglas B. Ham & Stephen Lockwood, Parsons Brinckerhoff (PB), Spring Park Technology Center with Science Applications International Corporation (SAIC) Transportation Policy and Analysis Center, October 2002

Reference Documents (continued)

- FHWA, "Recommendations for Bridge and Tunnel Security", 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

- "Terrorism and the Security of Public Surface Transportation", RAND Corporation, Brian Michael Jenkins, CT-226, April 2004, Testimony presented to the Senate Committee on Judiciary on April 8, 2004, www.rand.org