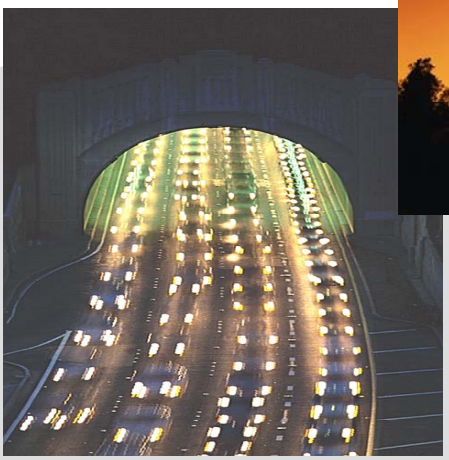
CONTRACTOR'S FINAL REPORT

A Guide to Highway Vulnerability Assessment

for Critical Asset Identification and Protection

Appendices A - F



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

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

Prepared by

Science Applications International Corporation (SAIC)
Transportation Policy and Analysis Center
7990 Science Applications Court
Vienna, VA 22182

May 2002

Table of Contents

ACKNOWLEDGMENT OF SPONSORSHIP

This work was sponsored by the American Association of State Highway and Transportation Officials, in cooperation with the Federal Highway Administration, under a grant from the National Cooperative Highway Research Program, which is administered by the Transportation Research Board of the National Research Council.

Appendix A: Background

The information in this section can be used in conjunction with the Introduction Section in the Guide.

Context of the Guide

Recent history shows that transportation systems are commonly targeted by terrorist organizations. According to Transportation Secretary Norman Y. Mineta,

> *"Terrorists attack transportation systems because they make attractive targets. Airplanes, buses, subways and cruise ships carry large numbers of people within concentrated, predictable areas and on set timetables. We design them to be convenient to the public. But, apart from the aviation security system, that also makes these common modes of transportation easily accessible to terrorists and their explosive devices or other weapons."* [1]

In its emergency planning guide to state and local governments, the Federal Emergency Management Agency (FEMA) identifies traffic, trucking and transportation activity, waterways, airports, trains/subways, and government facilities among a select listing of potential areas of vulnerability within the nation to terrorist attack[2].

To address these vulnerabilities, in May 1998, the Clinton Administration issued Presidential Decision Directive (PDD)-63, "Protecting America's Critical Infrastructures," to help strengthen the nation's defenses against terrorism and other unconventional threats. PDD-63 designates the U.S. Department of Transportation (USDOT) as the lead federal agency for protecting the nation's transportation infrastructure. Some of the possible threats facing the transportation infrastructure include:

- Terrorism
- Major criminal incidents
- Other event-related crimes
- Natural and technological disasters
- Public health emergencies
- Vehicle and pedestrian traffic problems
- Inadequate resources

The types of weapons that are of particular concern are those typically labeled as weapons of mass destruction (WMD). Under U.S. law, WMD are defined as:[3]

- Any destructive device including any explosive, incendiary, or poison gas:

[1] U.S. Department of Transportation. Statement of Norman Y. Mineta, Secretary of Transportation before the Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State and the Judiciary, on the Government's Efforts to Combat Terrorism. 08 May 2001. Found on the Internet at: http://www.senate.gov/~appropriations/commerce/testimony/terrmine.htm.

[2] Federal Emergency Management Agency. "State and Local Guide for All-Hazard Emergency Operations Planning." SLG-101. April 2001.

[3] 18 USC Sections 2332a and 921(a)(4)(A)

  - Bomb
  - Grenade
  - Rocket having a propellant charge of more than four ounces
  - Missile having an explosive or incendiary charge of more than one-quarter ounce
  - Mine
  - Devices similar to any of the devices described above
- Any weapon that is designed or intended to cause death or bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors,
- Any weapon involving a disease organism, or
- Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Generally, WMD are divided into several categories:

- Chemical agents,
- Nuclear weapons,
- Biological agents,
- Radiological agents, and
- Conventional explosives.

Sometimes, the first four categories are referred to as "CNBR" weapons. Alternatively, nuclear, biological, and chemical weapons are called "NBC" weapons. As the threat of WMD terrorism increases, more time, attention and resources are being expended to define better what these weapons are and the threats they pose to the nation.

The use of WMD poses new and different threats to state agencies, including State Departments of Transportation. For years, states have dealt with multiple types of emergencies, the most far-reaching involving large natural disasters. In the aftermath of September 11th, State DOTs are now far more aware of the devastating consequences of terrorism. Below is a chart showing some of the similarities and differences between non-terrorist/non-WMD events and terrorist events where WMD is utilized:

Table 1: Shared and Specific Characteristics of Terrorist/WMD Events versus Non-Terrorist/Non-WMD Events[4]

Shared Characteristics	***Specific Characteristics of Terrorist/WMD Events***
• Mass casualties • Damage to infrastructure • With or without warning • Evacuation or displacement of citizens	• Caused by people on purpose • Will be treated as crime scenes • May not be immediately recognizable as terrorist events • May not be single events • Place responders at higher risk • May result in widespread contamination of critical equipment and facilities • May expand geometrically in scope • May cause strong public reaction • Targets a facility's weakness

Different WMD may yield different consequences to people and property, as highlighted below.

Table 2: Possible Consequences of a WMD Event

WMD		***Possible Consequences***
Conventional Explosives (e.g., detonation of fuel oil-fertilizer bomb, military-type explosives, etc.)	⇨	• Casualties • Impacts mostly local to explosion • Structural collapses • Exposure to dust and hazardous building materials, e.g., asbestos • May be used to spread harmful radiological or chemical materials
Chemical (e.g., dispersion of pesticides, mustard gas, chlorine gas, cyanide, tear gas, etc.)	⇨	• Unexplained deaths and illness • Impacts mostly local to release but may be some distribution via, e.g., wind beyond release site • May be marked by unusual clouds, haze, mist, odors, tastes, droplets, etc. • May be persistent in environment
Biological (e.g., dispersion of viruses, bacteria, toxins, fungus, etc.)	⇨	• Unexplained deaths and illness possibly beginning a day or more after an event • Immediate impacts mostly local to release but may be expanded distribution through human transmittal • Possible persistence in environment • Possible geographic contamination

[4] Adapted from FEMA Web Site, Senior Officials' Workshop on Weapons of Mass Destruction

WMD		*Possible Consequences*
Radiological (e.g., dispersion of radioactive material by non-nuclear explosion or pressurized gas)	⇨	• Unexplained deaths and illness • Impacts mostly local to release but may be some distribution beyond release site by wind • Persistence in environment • Geographic contamination Also: • Conventional explosives used for dispersal may also cause impacts
Nuclear (e.g., nuclear detonation with radioactive fallout)	⇨	• Casualties • Large-scale infrastructure destruction • Extensive radioactive fallout • Long-term persistence in environment • Geographic contamination

Methodology for developing this Guide

In 2001, AASHTO surveyed its members and identified thirty-two State DOTs that would share information about their vulnerability assessment plans. The research team responsible for authoring this Guide contacted representatives from all of the identified agencies, requesting their cooperation in providing information and documentation. Phone interviews were conducted with twenty-four states that responded favorably to this request. During these telephone interviews, the research team discussed the status of each agency's vulnerability assessment plan and requested copies of documentation (i.e., lessons learned, case studies, memoranda of agreement, mutual aid agreement) that describe how the State DOTs assess vulnerability and develop, evaluate, and implement countermeasures. Lists of the documents collected, in either electronic or paper formats, and the individuals interviewed are provided in Appendices C and D, respectively.

Fourteen states provided written documentation and information. Three states (Utah, Kansas, and Alaska) could not disseminate their vulnerability assessments publicly. For those states, general information was collected from interviews or other sources.

As the interviews with states progressed, the research team found few State DOTs with practical vulnerability assessment experience, which hindered compiling an extensive list of "best practices." As a result, the research team pursued federal and international sources to augment the information obtained from State DOTs.

The research team contacted and collected open source information from USDOT and other federal agencies either directly or through secondary sources (e.g., subject-matter experts and FHWA contacts). Information was collected from the following USDOT agencies: Federal Transit Administration, Federal Aviation Administration, U.S. Coast Guard, and the Volpe National

Transportation Systems Center (part of the Research and Special Programs Administration). The research team examined secondary resources for information from other federal agencies, including the U.S. Department of Defense (especially the Defense Threat Reduction Agency), the U.S. Department of Justice, and the Federal Emergency Management Agency, among others.

The research team sought information from several European countries and Israel because of these countries' experience in dealing with terrorist attacks. The team identified contacts in European countries through the FHWA Office of International Programs and through Internet searches. The team contacted nine European countries via telephone calls and e-mails, seeking answers to the same questions posed to the State DOTs. Several of the countries do not have any vulnerability assessment plans and only Norway provided a document, printed in 1995, with guidelines for municipal risk and vulnerability analysis. Several other documents were obtained from a European Union website and are cited in the bibliography to this Guide (Appendix D).

A summary of the sources contacted for the project is indicated below:

SOURCE	NUMBER
States contacted based on AASHTO's survey indicating willingness to share vulnerability assessment plans	32
States that discussed their plans in phone interviews	24
States that provided vulnerability assessment and various related documentation	14
Federal resources with related vulnerability assessment information	6
Federal resources referenced with applicable vulnerability assessment methodologies available for public viewing	3
Foreign countries contacted	10
Foreign countries that provided documentation (another provided information to FHWA that could not be released)	1

The vulnerability assessment method presented in this Guide is derived from a careful review of the compiled state, federal, and international interview findings and documentation received. Many examples cited in the Guide are from state and federal processes. A summary of methodologies from all the documentation is provided in Appendix F.

The research team either implicitly or explicitly applied the following criteria in selecting preferred approaches to be included in the Guide:

- *Available/Accessible* – Is the approach generally available to State DOTs (e.g., non-proprietary, unclassified, in the public domain)?
- *Transparent* – Is the approach relatively easy to understand for those likely to be applying it? Are there theoretical underpinnings that many State DOTs will find difficult to understand or accept?
- *Replicable* – When the approach is repeated under similar conditions, will similar results be obtained?

- *Reasonable* – Are the resulting vulnerability assessments consistent with "good judgment" – do they meet the "prudent and reasonable person" test?
- *Scalable* – Is the approach limited in terms of the number of assets that could be considered or can it be applied in both small and large states (i.e., those with few assets and those with many)?
- *Robust* – Is the approach highly restricted to specific asset types (e.g., geometries, locations, loads, designs) and threat situations or can it be applied across a broad range of asset types and scenarios?
- *Cost-Effective* – Are the resources required to implement the approach commensurate with the value of the results to State DOTs?
- *Modular/Incremental* – Does the approach support an evolutionary approach in which State DOTs can begin with selected critical assets and expand the number and scope of the assets over time without losing the value of the initial assessment?

Appendix B: Worksheets

The worksheets in this appendix are exact copies of the worksheets from the Guide to Highway Vulnerability Assessment. They are provided in this section for easy reference. Full description of these worksheets is provided in the Guide.

Worksheet 1: Critical Asset Factors Values and Scoring

CRITICAL ASSET FACTOR	VALUE	DESCRIPTION
Deter/Defend Factors		
A) Ability to Provide Protection	1	Is there a system of measures to protect the asset?
B) Relative Vulnerability to Attack	2	Is the asset relatively vulnerable to an attack? (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 action 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 maintaining government continuity?
I) Military Importance	5	Is the asset important to military functions?
Consequences to the General Public		
J) Available Alternate	4	Is there a substitute that is designated to take the place of the asset, if necessary, to perform the same or similar duties? (i.e., Is there another bridge that crosses the river in a nearby location that could be used if the main bridge 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?

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															

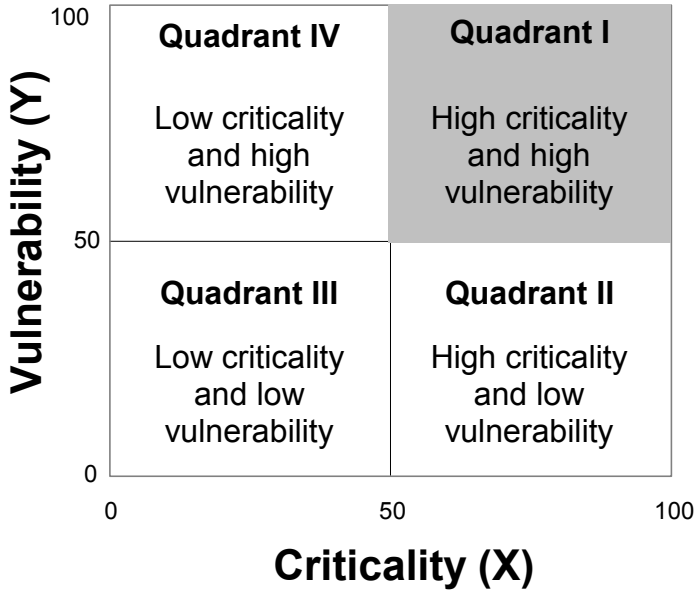
Worksheet 3: Vulnerability Factors and Scoring

VULNERABILITY FACTOR	*FIRST SUB-ELEMENT*	*SECOND SUB-ELEMENT*
Visibility and Attendance	Level of Recognition (A)	Attendance/Users (B)
Access to the Asset	Access Proximity (C)	Security Level (D)
Site Specific Hazards	Receptor Impacts (E)	Volume (F)

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

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												

Worksheet 4: Consequence Assessment



Worksheet 5: Countermeasure Identification

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

Worksheet 6: Countermeasure Costs

	Sample Countermeasure Relative Cost Range		
	Capital Investment	**Annual Operating Cost**	**Annual Maintenance Cost**
L	<$100K	<$50K	<$25K
M	$100K to $500K	$50K to $250K	$25K to $100K
H	>$500K	>$250K	>$100K

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.						
Institute full-time surveillance at the most critical assets where alternate routes are limited or have not been identified.						
Eliminate parking under any of the most critical type bridges. Elimination of the parking can be accomplished through the use of concrete barriers.						
Place barriers in such a way as to eliminate ease of access where a vehicle could be driven right up to the asset.						
Install security systems with video capability at all DOT facilities.						
Protect ventilation intakes with barriers.						
Install and protect ventilation emergency shut off systems.						
Install Mylar sheeting on inside of windows to protect employees from flying glass in the case of an explosion.						
Place a full-time security officer in a guard shack to control access.						
Lock all access gates and install remote controlled gates where necessary.						
Develop and implement a department-wide security policy.						
Limit access to all buildings through the issuance of a security badge with specific accesses identified and controlled through the card.						
Train all DOT personnel to be more observant of their surroundings and potentially dangerous packages, boxes, people, etc.						
Improve lighting.						
Increase surveillance at tunnels by installing cameras linked to the TOC.						
Add motion sensors to fences.						

OPERATIONAL SECURITY PLAN OUTLINE

Copy No. _____ **Issuing Department: _____**
Place of Issue: _____ **Date of Issue: _____**

1. **Purpose.** State the plan's purpose.
2. **Area Security.** Define the assets considered critical and establish priorities for their protection.
3. **Access Restrictions.** Define and establish restrictions on access and movement into critical areas. Categorize restrictions to personnel, materials, and vehicles.
   - 3.1. Personnel restriction
     - 3.1.1. Authority for access
     - 3.1.2. Criteria for access
     - 3.1.3. Employees
     - 3.1.4. Visitors
     - 3.1.5. Contractors
     - 3.1.6. Vendors
     - 3.1.7. Emergency responders
     - 3.1.8. National guard
   - 3.2. Material restrictions
     - 3.2.1. Requirements for admission of material and supplies
     - 3.2.2. Search and inspection of material for possible sabotage hazards
     - 3.2.3. Special controls on delivery of supplies or personal shipments in restricted areas
   - 3.3. Vehicle restrictions
     - 3.3.1. Policy on search of departmental and privately-owned vehicles, parking regulations, controls for entrance into restricted and administrative areas:
       - 3.3.1.1. Departmental vehicles
       - 3.3.1.2. POVs
       - 3.3.1.3. Emergency vehicles
       - 3.3.1.4. Vehicle registration
4. **Countermeasures**. Indicate the manner in which the following countermeasures will be implemented on the installation.
   - 4.1. Protective barriers:
     - 4.1.1. Definition
     - 4.1.2. Clear zones
     - 4.1.3. Criteria
     - 4.1.4. Maintenance
   - 4.2. Signs
     - 4.2.1. Types
     - 4.2.2. Posting
   - 4.3. Gates
     - 4.3.1. Hours of operation
     - 4.3.2. Security requirements
     - 4.3.3. Lock security
   - 4.4. Barrier plan
     - 4.4.1. Protective lighting system
     - 4.4.2. Use and control
     - 4.4.3. Inspection
     - 4.4.4. Action taken in case of commercial power failure
     - 4.4.5. Action taken in case of failure of alternate power source

- 4.5. Emergency lighting system
  - 4.5.1. Stationary
  - 4.5.2. Portable
- 4.6. Intrusion Detection System
  - 4.6.1. Security classification
  - 4.6.2. Inspection
  - 4.6.3. Use and monitoring
  - 4.6.4. Action taken in case of alarm conditions
  - 4.6.5. Maintenance
  - 4.6.6. Alarm logs or registers
  - 4.6.7. Tamper-proof provisions
  - 4.6.8. Monitor-panel locations
- 4.7. Communications
  - 4.7.1. Locations
  - 4.7.2. Use
  - 4.7.3. Tests
  - 4.7.4. Authentication
- 4.8. Security personnel. General instructions that would apply to all security personnel
  - 4.8.1. Detailed instructions such as special orders and procedural information should be attached as annexes
  - 4.8.2. Security personnel include
    - 4.8.2.1. Composition and organization
    - 4.8.2.2. Length of assignment
    - 4.8.2.3. Essential posts and routes
    - 4.8.2.4. Weapons and equipment
    - 4.8.2.5. Training
    - 4.8.2.6. Method of challenging with signs and countersigns
    - 4.8.2.7. Integrating with the local incident command system

5. **Contingency planning**. Required actions in response to various emergency situations.
   - 5.1. Detailed plans for situations (counter terrorism, bomb threats, hostage negotiations, disaster, fire, and so forth) should be attached as annexes)
     - 5.1.1. Individual actions
     - 5.1.2. Management actions
     - 5.1.3. Security actions

Appendix C: Acronym List

AASHTO	American Association of State Highway and Transportation Officials
ADT	Average Daily Traffic
APTA	American Public Transportation Association
BNICE	Biological, Nuclear/Radiological, Incendiary, Chemical, Explosive agents
CCTV	Closed Circuit Television
CNBR	Chemical agents, Nuclear weapons, Biological agents, Radiological agents, and Conventional explosives
DOJ	(U.S.) Department of Justice
DOT	(U.S.) Department of Transportation
DPW	Department of Public Works
FAA	Federal Aviation Administration
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FTA	Federal Transit Administration
HAZMAT	Hazardous Material
NBC	Nuclear, Biological, Chemical
NCHRP	National Cooperative Highway Research Program
POV	Privately Owned Vehicle
PTE	Potential Threat Element
SAIC	Science Applications International Corporation
TOC	Traffic Operations Center
USCG	United States Coast Guard
WMD	Weapons of Mass Destruction

Appendix D: Bibliography

Arkansas

1. *Evaluation of the Most Critical Bridges In Arkansas for Vulnerability From Terrorists*. (2001, November 13)
2. *Security Measures For Critical State Highway Bridges*. (Excel Spreadsheet)

California

3. *Bridge Vulnerability Assessment*
4. Governor's Office of Emergency Services. *California Terrorism Response Plan*. (2001, February 1). Found on the Internet at http://www.bsa.ca.gov/lhcdir/disaster/StateTerrorismPlan.pdf
5. *Critical Structure Priorities*
6. Mineta Transportation Institute, San Jose State University. *Protecting Public Surface Transportation Against Terrorism and Serious Crime: An Executive Overview*. MTI Report 01-14. (2001, October)
7. *Response to LAO Security Inquiry*

Illinois

8. Illinois Department of Transportation & State Police. *Duty Officer Manual, Appendix A, Joint Operational Policy Statement*. (1999, March 1)
9. Illinois Department of Transportation, Bureau of Operations. *Earthquake Preparedness Plan*. (2001, March 15)
10. Illinois Department of Transportation, Bureau of Operations. *Emergency Operations Manual*. (1992, November 18)
11. *Illinois Contingency Planning*. (2001, September 18)
12. Illinois Emergency Management Agency. *Illinois Emergency Operations Plan.* (1998, May 1)

Iowa

13. Office of the Homeland Security Advisor. *Assessment Checklist & Threat Advisory Recommendations*
14. *Cass County Hazard Analysis*. (1998, October 1). Found on the Internet at http://www.metc.net/cassema/Hazard%20Analysis.htm
15. Office of the Homeland Security Advisor. *Iowa's Critical Asset Assessment Model* (2002)
16. Office of the Homeland Security Advisor. *Iowa's Homeland Security Critical Asset Assessment Model (CAAM)*
17. Office of the Homeland Security Advisor. *Threat Advisory Recommendations*

Kentucky

18. The Patterson School, National Security Working Group. *Weapons of Mass Destruction Needs Assessment*.

Maryland

19. Igbinosun, Egua U., MD State Highway Administration. *Transportation-Related Emergency Preparedness & Security Measures*. (2002, February 12)

New Mexico

20. New Mexico Surety Task Force. *Integrated Transportation Analysis: Framework For Response To Malevolent Attack*. (2002, February 1)
21. New Mexico Surety Task Force. *Integrated Transportation Analysis Vulnerability Assessment: General Description*. (2002, January 1)
22. New Mexico Surety Task Force. *Standard Operating Procedures for Security*. (2002, January 1)
23. New Mexico State Highway & Transportation Department. *Surety Task Force Video Presentation Script*. (2002, February 4)

New York

24. New York Department of Transportation. *New York Department of Transportation Manual of Administrative Procedures 6.0-13 Emergency Management*. (1995, March 29)
25. New York Department of Transportation. *Transportation Assets Security Report*
26. Transportation Management Center. *Transportation Security Task Force Review*. (2002, March 1)

Oregon

27. EAI Corporation. *Jurisdictional Support Package for Oregon Domestic Preparedness Statewide Needs Assessment.* (2001, February 6)
28. Oregon Department of Transportation, Transportation Operations Center Managers Group. *Oregon Department of Transportation Primary/Alternate TOCs for Warning Functions*. (2000, November 1)
29. Oregon Department of Transportation. *Oregon Department of Transportation Emergency Operations Plan*. (2002, February 1)
30. CH2MHILL. *Prioritization of Oregon Bridges for Seismic Retrofit* . (1997, January 1)

South Carolina

31. South Carolina Emergency Preparedness Division – Homepage. Found on the Internet at http://www.state.sc.us/epd/library/index.htm

Texas

32. Governor's Task Force on Homeland Security. Found on the Internet at http://www.governor.state.tx.us/homelandsecurity/index.htm
33. Roy Robinson, Texas A&M University System, National Emergency Response and Rescue Training Center. *Public Works: Preparing for and Responding to Terrorism/Weapons of Mass Destruction*.
34. Mary Lou Ralls, Texas Department of Transportation. *Security Activities Related to Texas Bridges*. 2002 TRB Annual Meeting. (2002, January 13)
35. Mary Lou Ralls, Texas Department of Transportation. *Texas Department of Transportation Methodology for Identifying Critical Assets.* (2002, April 19)

Virginia

36. Virginia Department of Transportation, Red Team. *Facility Security and Anti-Terrorism, Awareness and Preparedness & Risk and Vulnerability Assessment*. (2002, March 22)
37. *Incident Management Update*. (2001, November 1)

38. Virginia Department of Transportation, Red Team. *Manual #1*. (1999, April through 2001, December)
39. Mike McAllister, Central Office & Districts. *Physical Security Assessment*. Virginia Department of Transportation Red Team Meeting. (2001, November 30)
40. Virginia Department of Transportation. *Protection of Infrastructure*. (2001, November 6)
41. Metro IT Solutions. *Recovery Requirements*. (2002, January 16)
42. Center for Risk Management of Engineering Systems, University of Virginia. *Risk-Based Critical Infrastructure Protection For Virginia State Police and Virginia Localities*. (2002, January 20)
43. Center for Risk Management of Engineering Systems, University of Virginia. *Risk-Based Post-Hurricane Recovery of Highway Signs, Signals, and Lights - Final Report*. (1998, April 29)
44. Center for Risk Management of Engineering Systems, University of Virginia. *Risk-Based Post-Hurricane Recovery of Highway Signs, Signals, and Lights - Progress Report*. (1999, May 7)
45. Virginia Department of Transportation, Red Team. *Security and Anti-Terrorism, Building Security: An Architect's Guide*. (1998, June 5)
46. Virginia Department of Transportation. *Security Awareness Guide*. (2002, February 14)
47. *Summary of Lessons Learned from Pentagon Attack*
48. Virginia Department of Transportation. *VDOT Infrastructure Physical Security Enhancement Program (VISPSEP)*. (2002, March 12)
49. Perry Cogburn, Virginia Department of Emergency Services. *Virginia Emergency Operations Plan Volume 7*. (2000, July 1)
50. Virginia Department of Emergency Services. *Virginia Emergency Operations Plan Volume 8, Terrorism Consequence Management*. (1999, May 22)
51. Members of Virginia Governor's Domestic Preparedness Working Group. *Virginia's Critical Transportation Infrastructure Protection: Risk Assessment Study*

Washington

52. E.H. Henley, Washington Department of Transportation. *Bridge Seismic Retrofit Program Report*. (1993, September 1)
53. Washington Department of Transportation, Field Operations Support Service Center. *Disaster Plan*. (1999, June 1)
54. Stephanie Tax, Washington Department of Transportation. *Public Works Emergency Response Mutual Aid Agreement*. (2001, January 12)
55. Washington Department of Transportation. *Washington State Department of Transportation Year 2000 Contingency Plan* . (1999, April 30)
56. Terry Simmonds, Washington Department of Transportation. *The 2001 Nisqually Earthquake - Lessons Learned*. (2001, October 1)

Washington, D.C.

57. Risk Threat Assessment Working Group. *Risk Threat Assessment Working Groups Meeting Minutes*. (2001, November 1)
58. Risk Threat Assessment Working Group. *Risk Threat Assessment Working Groups Meeting Minutes*. (2001, November 8)

59. Risk Threat Assessment Working Group. *Risk Threat Assessment Working Groups Meeting Minutes*

Wisconsin

60. Wisconsin State Patrol. *State Employee and Building Security Plan*. (2001, October 8)

United States Department of Transportation

61. John Veatch, Joseph James, Terry May, Thomas Wood, Eric Kruse – Science Applications International Corporation (SAIC). *Airport Vulnerability Assessment Methodology*. (1999, October 5)
62. U.S. Department of Transportation. *Improving Surface Transportation Security: A Research and Development Strategy.*
63. John A. Volpe National Transportation Systems Center. *Surface Transportation Vulnerability Assessment*. (2001, January 25)
64. Federal Transit Administration. *Transit Threat and Vulnerability Assessment Methodology*
65. John A. Volpe National Transportation Systems Center. *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.* (2001, August 29)

Other United States Federal Agencies

66. U.S. Department of Energy. *A Comprehensive Emergency Management System*. USDOE Order O 151.1. (2000, November 1)
67. Debbie Gallo, US Air Force. *Air Force Vulnerability Assessments*. (2001, March 1)
68. John Sorensen. *An Approach for Deriving Emergency Planning Zones for Chemical Weapons Emergencies*. (1992, January 1)
69. Antiterrorism Assessment Division, Defense Threat Reduction Agency. *AT/FP Program Overview.*
70. U.S. Department of Energy. *Emergency Management Guide*. USDOE G 151.1-1. (1997, August 21). Found on the Internet at http://www.infowar.com/civil_de/slg101.pdf
71. Department of Justice, Office of Justice Programs. *Emergency Response To Terrorism, Self-Study*. (1999, June)
72. Department of Justice, Office for State & Local Domestic Preparedness Support. *Fiscal Year 1999 State Domestic Preparedness Support Program*. (2000, May 15)
73. White House Office of the Press Secretary. *Governor Ridge Announces Homeland Security Advisory System*. (2002, March 12). Found on the Internet at http://www.whitehouse.gov/news/releases/2002/03/20020312-1.html.
74. Federal Emergency Management Agency. *Guide for All-Hazard Emergency Operations Planning (SLG-101).* (1996, September 1)
75. United States Transportation Command. *Integrated Vulnerability Assessment Integrated Process Team.* (2001, March 1)

European Union

76. A.L.C. Roelen, National Aerospace Laboratory. *A Cost Benefit Analysis of Wake Vortex Measures*. (2001, November 1)

77. Roger Steen, Directorate for Civil Defense & Emergency Planning. *A Guide to Information Preparedness*. (2000, April 1). Found on the Internet at http://www.dsb.no/presentation/index.asp
78. A.L.C. Roelen, National Aerospace Laboratory. *Costs of Safety Measures and Regulation*. (2001, July 1)
79. Wouter van Dijk, Roelof Jan Molemaker. *The Cost of Unsafety*. (2001, March 1)
80. A.L.C. Roelen, National Aerospace Laboratory. *Development of a Scenario-Based Methodology to Assess Safety Levels Within the Aviation System and to Determine the Effect of Changes on the Level of Safety*. (2001, October 1)
81. Directorate for Civil Defense and Emergency Planning. *Guidelines for Emergency Planning for Ministries and Central Government Agencies*. (1999, January 1), available on the Internet at http://www.dsb.no/presentation/index.asp
82. Directorate for Civil Defense and Emergency Planning. *Guidelines For Municipal Risk And Vulnerability Analysis*. (1995, January 1)
83. A.L.C. Roelen, R. Piers, R.J. Molemaker, P. Hayes. *Handbook for Conducting Cost Benefit Analysis of Safety Measures in Air Transport*. (2001, December 1)
84. Roger Steen, Directorate for Civil Defense & Emergency Planning. *Risk Assessment in Europe*. A Summary from the EU Workshop on Risk Assessment. (1999, November 25). Found on the Internet at http://www.dsb.no/presentation/index.asp

Appendix E – List of Individuals Contacted

Alaska Department of Transportation	Frank Richards
Arkansas Department of Transportation	Ralph J. Hall
California Department of Transportation	John Cottier, Steve, Vaughn, George Whitney
Colorado Department of Transportation	Tom Norton
Florida Department of Transportation	Derrick Jenkins
Illinois Department of Transportation	Dave Johnson
Iowa Department of Transportation	Ray Callahan
Iowa Emergency Management Division	Aaron Mumm, Brady Robbins
Iowa Technology Department	Larry Brennan
Kansas Department of Transportation	Susan F. Barker
Kentucky Department of Transportation	Gary Mitchell
Louisiana Department of Transportation	Joe Modicut, Sean Fontenot
Maryland Department of Transportation	Francis McGrath, Tom Hicks, Tom Wilson, Bob French, Egua Igbinosun, Linda Singer, Fran McGrath, Dan Hering, Tim Watson, John Scally, John Contestabile
Massachusetts Department of Transportation	Steve Pepin
Nebraska Department of Transportation	Dale Dvorak
Nevada Department of Transportation	Frank Taylor
New Hampshire Department of Transportation	Carol Murray
New Jersey Department of Transportation	F. Rodney Roberson
New Mexico Department of Transportation	David Albright
New York Department of Transportation	Jack Williams
New York/New Jersey Port Authority	Mike Eadiciccio
North Carolina Department of Transportation	Mrinmay Biswas
North Dakota Department of Transportation	Jerome Horner
Oklahoma Department of Transportation	Bill Miller
Oregon Department of Transportation	Rose Gentry
South Carolina Department of Transportation	Carl Chase Jr
Tennessee Department of Transportation	Jim Jeffers, Carl Cobble
Texas Department of Transportation	Jim Daily, Mary Lou Ralls, Ed Wueste
Utah Department of Transportation	Neal Christensen
Virginia Department of Transportation	Steve Mondul, Perry Cogburn, Mike McAllister
Washington D.C. Department of Transportation	Natalie Jones
Washington Department of Transportation	Terry Simmonds
West Virginia Department of Transportation	James L. Riggs
Wisconsin Department of Transportation	Douglas L. Van Buren, Bob Phasic
Wyoming Department of Transportation	Kenneth Shultz, P.E.
U.S. Department of Transportation	Hana Meier, George Romack, Vince Pearce, Pat Hasson, Michael Dinning
Military Traffic Management Command	Dave Dorfman
Embassy of Germany	Karen Kammann Klippstein
Embassy of Italy	Gabriella Navarra
European Union	Alfred Roelen
Swedish Road Administration	Thomas Lange
Swiss Federal Road Authority	Michael Gehrken
Transport Canada	Amanda Williams

Appendix F: Illustrative Practices

This section provides samples of the vulnerability assessment methods practiced by state and federal agencies, and are not the complete methodology of the respective agency. For complete methodologies please reference the original documents.

Critical Assets Identification

Practice

Arkansas[1], Maryland[19] and the U.S. Department of Justice[72] (USDOJ) each documented critical assets but did not provide the documented process used to derive these assets. Washington[52], Oregon[30], Iowa[16] and Texas[34] each documented the process used to identify an asset as "critical". Each use either a quantitative (assigned numeric value) or high, low, medium system. The Federal Aviation Administration[61] identifies critical assets through a calculation of "threat analysis" and "consequences" (each of which are derived through quantitative methods).

Iowa

(Reference 16, *Iowa homeland Security Critical Asset Assessment Model - CAAM)*

The criticality assessment is a process designed to systematically identify and evaluate important systems and infrastructure as it relates to the factors in the table below. Each of the sub-elements is given a score based on a scale of 1 through 5 dependent upon specific criteria. The criticality subtotal is converted to a percentage and then graphed along the X-axis of a coordinate system.

Criticality Elements	Sub-element		Sub-element	Element Subtotal
Mass Casualty Risk	Effect (1-5)	X	Severity (1-5)	1-25
Emergency Response Function	Time loss (1-5)	X	Jurisdiction Population (1-5)	1-25
Economic Impact	Scope (1-5)	X	Impact (1-5)	1-25
Key Military Installations	Time loss (1-5)	X	Facility Function (1-5)	1-25
Critical Infrastructure	Time loss (1-5)	X	Population Impacted (1-5)	1-25
Continuity of Government	Time loss (1-5)	X	Population Impacted (1-5)	1-25
Symbolic Asset	Time loss (1-5)	X	Level of recognition (1-5)	1-25
Criticality Subtotal (x)				**7-175**

Oregon
(Reference 30, *Prioritization of Oregon Bridges for Seismic Retrofit*)

Pages 11-12 discuss criticality functions. These functions represent the socioeconomic implications of losing service of a particular structure because of an earthquake. (can be applied to terrorist attacks)

Appendix B describes the priority, vulnerability and criticality rankings in more detail and describes the equations used to derive the index.

Page 9 of the document shows a table with seismic prioritization model vulnerability groups. Those with unstable bearings are the most vulnerable.

Texas
(Reference 34, *Security Activities Related to Texas Bridges*)

Texas Responses to Factors for Identifying Critical Transportation Infrastructure Assets on November 2001 AASHTO/TRB transportation security survey
Rated from Extremely Important (5) to Less Important (1)

5 - Impact on Local, State, and National Economy
5 - Major Commercial Route
4 - Major Passenger Route
3 - Cost to Repair or Replace
3 - Time to Repair or Replace
2 - Relative Vulnerability to Attack
1 - Ability to Provide Adequate Protection
1 - Symbolic Nature of the Target

Washington State
(Reference 52, *Bridge Seismic Retrofit Program Report*, pp. 11-15)

Prioritization of retrofit needs:

Superstructure Group	**Type of Deficiency**
1	Bridges with in-span hinges.
2	Bridges simply supported at piers.
Substructure Group	
3	Bridges with single-column piers.
4	Bridges with multi-column piers having 3 or more types of substructure deficiencies.
5	Bridges with multi-column piers having 3 or more types of substructure deficiencies.
Priority Group	
S	Bridges that require further structural analysis to assess whether seismic retrofit is warranted. These are essentially large or unusual type structures. Double-deck bridges are included in this category.

Vulnerabilities Assessment

Part I - Characterize the threat

Practice

Maryland[19], U.S. Coast Guard, and the Federal Aviation Administration[61] each documented a quantitative method to derive threat analysis. The method most often performed was assigning and summing numeric values to multiple attributes (existence, history, capability, etc.) to the threat (e.g., 1 – not attractive, 5 – extremely attractive).

Maryland

(Reference 19, *Transportation-Related Emergency Preparedness & Security Measures*)

MDOT operates within a 5-tier Threat Condition Response System:

Level 1: Weapons of Mass Destruction (WMD)
Level 2: Credible Threat
Level 3: Potential Threat
Level 4: Minimal Threat
Level 5: No Threat

Federal Aviation Administration

(Reference 61, *Airport Vulnerability Assessment Methodology*, p. 3)

Target Attractiveness

Attractiveness Rating	Value	Typical Examples
Extremely Attractive	5	Aircraft with passengers and an identified threat or an air carrier with an identified threat.
Very Attractive	4	Aircraft with passengers or an operational terminal.
Attractive	3	Passenger aircraft without passengers or support services essential for operations.
Less Attractive	2	An in-service cargo aircraft or retail operations.
Unattractive	1	Out of service aircraft.

U.S. Department of Justice

(Reference 72, *Fiscal Year 1999 State Domestic Preparedness Support Program*)

THREAT FACTOR VALUES

THREAT FACTOR	VALUE
Existence	1
History	1
Intentions	2
Capability	2
Targeting	4

Table 2-b-1

If the information known to the assessment group does not satisfy the parameters set forth in the definition of any one factor, or the information is not credible, then that factor cannot be included in the valuation process. Examples are charted below:

EXAMPLE THREAT LEVEL ASSESSMENT

Identity of PTE	Existence (1)	Violent History (1)	Intentions (2)	WMD Capability (2)	Targeting (4)	PTE THREAT LEVEL
Example 1	1					1
Example 2	1		2			3
Example 3	1		2	2	4	9
Example 4	1	1		2		4
Example 5	1	1	2	2	4	10
X = FACTORS FOUND TO BE PRESENT						

Table 2-b-2

Part II - Assign vulnerability factors to the critical assets

Practice

Washington[52], Oregon[30], New Mexico[21], Iowa[16], Texas[35], Arkansas[1], U.S. Coast Guard, U.S. Department of Justice[72] and the Federal Aviation Administration[61] each documented some method to perform the vulnerability assessment. Methods of assessing vulnerability include:

- Assigning numeric values (ex: 1 – "not vulnerable," 5 – "extremely vulnerable") to one or more attributes (visibility, value, access, etc.)
- An equation analyzing current security of the facility
- An equation analyzing current accessibility of the facility
- On-site photos with a professional opinion of each vulnerable point of a facility

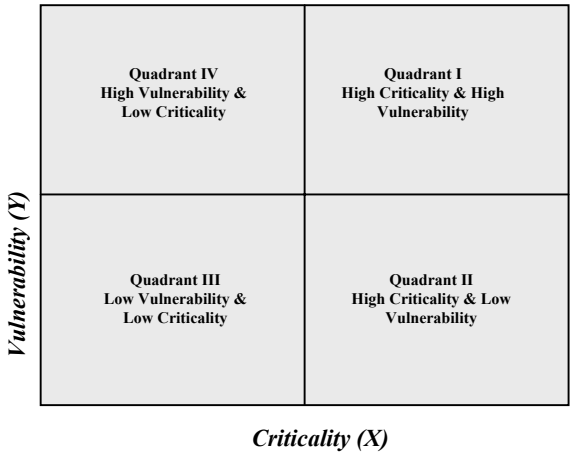
Iowa

(Reference 16, *Iowa Homeland Security Critical Asset Assessment Model - CAAM*)

The vulnerability assessment is a process designed to systematically identify and evaluate important systems and infrastructure as it relates to the factors in the table below. The process identifies exposures in physical structures, personnel protection systems, and production processes. Each of the sub-elements is given a score based on a scale of 1 through 5 dependent upon specific criteria. The vulnerability subtotal is converted to a percentage and then graphed along the Y-axis of a coordinate system.

Vulnerability Elements	**Sub-element**		**Sub-element**	**Element Subtotal**
Visibility and Attendance	Level of recognition (1-5)	X	Attendance (1-5)	1-25
Access to the Asset	Access Proximity (1-5)	X	Security Level (1-5)	1-25
Site Specific Hazards	Receptor Impacts (1-5)	X	Volume (1-5)	1-25
Vulnerability Subtotal (y)				**3-75**

Asset Score = [Criticality, Vulnerability] = [((x/175)*100), ((y/75)*100)] = [X, Y]



New Mexico

(Reference 21, *Integrated Transportation Analysis Vulnerability Assessment: General Description*)

The ITA vulnerability assessment incorporates scenarios, tabletop exercises, emergency response and related training exercises to address potential targets, weapons and consequences.

The scenarios are designed to identify and then respond to significant and rare events that can occur due to terrorist attacks. The scenarios can be used to prevent incidents or mitigate results of an incident. Figure 4 on page 10 depicts the scenario development process.

A key point is made that vulnerability assessments are not one-time activities, but are an ongoing part of the transportation sector's responsibilities.

Figure 6 on page 13 depicts the ITA Vulnerability Assessment Flow Diagram. The process begins with the Surety Task Force definition of a major consequence. The FHWA, in cooperation with the NM State Highway and Transportation Dept., identifies critical infrastructure for the State of New Mexico. This identification of critical infrastructure may lead to changes in the major consequence definition as indicated by the two-way arrow in the diagram. The red team develops the scenarios and the blue team plans responses to the scenarios through operational plans. As the scenario process proceeds, the teams may change what is determined to be critical infrastructure. Response planning assists in determining how to harden critical infrastructure. Hardening is how existing resources are pre-deployed, or how the current transportation infrastructure is modified to make it more difficult for a person to use the infrastructure as a weapon or to have it be a target of an attack. The vulnerability assessment process can suggest design changes for new construction to ensure that critical infrastructure is adequately hardened. The outcome f the vulnerability assessment process is clear operational plans to be used by

emergency response personnel and other decision makers in the event of a malevolent attack or other incident with consequences.

Oregon
(Reference 30, *Prioritization of Oregon bridges for Seismic Retrofit*)

Pages 12 – 13 discuss the vulnerability function (V). However, this applies more to vulnerability to earthquakes than to terrorist attacks.

Texas
(Reference 35, Texas Department of Transportation *Methodology for Identifying Critical Assets*)

TxDOT utilizes a two-step process in determining the ranking of critical assets (bridges) across the state. The first step is an automated ranking of all the bridges listed in the National Bridge Inventory for the state. This ranking is done through the use a Microsoft Access program using a Texas Bridge Criticality Formula described below. The formula accounts for several criteria, such as Commerce, Transportation Needs, Navigational Access, etc. These criteria are measured using data available from the Bridge Inspection Data Base (BIDB) which can be downloaded to the Access program. As part of the formula, the relative importance given to each criterion can be adjusted by the use of a weighting factor to reflect the value TxDOT assigns to each different criterion.

The second step of the procedure involves incorporating the addition of other bridges to list based on the input from our various district offices around the state. These additions are necessary to account for specific site conditions that cannot be accounted for in the information available in the Bridge Inspection Data Base.

The structures that are obtained from the two processes are then combined into a final listing of critical bridges. This listing can then be used as the basis of further analysis for threats, vulnerabilities and possible countermeasures.

Texas Bridge Criticality Formula:

{[(Truck ADT x Truck ADT Factor / Max. Truck ADT) + (ADT x ADT Factor / Max. ADT) + (Detour x ADT x Detour Factor / Max. Detour x Max. ADT) + (Intersect Rt. ADT x Intersect Rt. Factor / Max. Intersect Rt. ADT) + (Interstate Intersection x Interstate Intersection Factor) + (Navigation Importance x Navigation Factor) + (International Importance x International Factor) + (Military Importance x Military Factor)] / 8} x Replacement Factor

Basic Elements of the Formula and their Definitions:

Commerce Criteria
Truck ADT = Average Daily Truck Traffic based on Item 109 of BIDB for the subject bridge.

Max. Truck ADT = The maximum Truck ADT for any bridge in the BIDB for the entire state.

Truck ADT Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Transportation Needs Criteria

ADT = Average Daily Traffic based on Item 29 of the BIDB.

Max. ADT = Maximum Truck ADT for any bridge in the BIDB for the entire state.

ADT Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Detour = Bypass, Detour Length based on Item 19 in the BIDB.

Max. Detour = Maximum Detour Length for any bridge in the BIDB for the entire state.

Detour Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Connectivity Criteria

Intersect Rt. ADT = Average Daily Traffic on the Intersecting Route

Max. Intersect Rt. ADT = Maximum Average Daily Traffic on the Intersecting route for any bridge in the BIDB for the entire state.

Intersect Rt. Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Interstate Intersection = 1 if both main and intersecting routes are Interstate Highways, or 0 if one or both are not Interstate Highways.

Interstate Intersection Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Navigational Access Criteria

Navigation Importance = 1 if the bridge requires a Coast Guard Permit based on Item 38 in the BIDB, or 0 if no Coast Guard permit is required.

Navigation Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

International Access Criteria

International Importance = 1 if the bridge borders on Mexico based on Item 98 on the BIDB, or 0 if it does not.

International Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Military Movement Criteria

Military Importance = 1 if the bridge is located on the Strategic Highway Network based on Item 100 in the BIDB, or 0 if it is not.

Military Factor = Numeric factor, nominally between 0 and 1, that relates the relative importance of this criterion to the other criteria in the formula.

Replacement /Repair Index

Replacement Factor = Structural Complexity x Span Length Factor, where:

Structural Complexity = one of three numeric factors based on if the superstructure type's complexity is rated low, medium or high. These numeric factors nominally range between 0 and 2. All bridge superstructure types from Item 43 of the BIDB were rated as being low, medium or high and the numeric factor are assigned accordingly.

Span Length Factor = one of three numeric factors based on the length of the main span of the bridge. These numeric factors nominally range between 0 and 2. Span lengths based on Item 48 of the BIDB are grouped as less than 150', 150' to 300' and more than 300', with numeric factors assigned accordingly.

Federal Transit Administration

(Reference 64, *Transit Threat and Vulnerability Assessment Methodology*, pp. 7-8)

Exhibit 4: Attack Vulnerability Levels

Description	Level	Ease Of Access
Very Easy	A	Very easy to access area or affect function undetected
Easy	B	Relatively easy to access area or function, no significant barriers to prevent
Difficult	C	Difficult to access area or function, various barriers in place
Very Difficult	D	Very difficult to access area or function, barriers very difficult to overcome
Too Much Effort	E	Extremely difficult and cumbersome to access area or function. No history of incursion or attempted incursion.

Federal Aviation Administration

(Reference 61, *Airport Vulnerability Assessment Methodology*, pp. 4-6)

Relative Risk

RR = TI (1-LA) (1-LS)
RR is relative risk;
TI is target importance (function of attractiveness and consequences);
LA is the likelihood of preventing an adversary attempt;
-Estimates are made for LA on a scale from *very high* (0.9) to *very low* (0.1)
(1-LA) is the likelihood that an adversary will make an attempt
LS is the likelihood of preventing success once an attempt is made; and
(1-LS) is the likelihood that an adversary will be successful, given an attempt has been made

LS Consists of two components:
Alert – the ability to detect and assess a malicious act.
Response – the ability to intercept and neutralize a malicious act.
-Estimates are made for the elements of LSA and LSR on a scale from *very high* (0.9) to *very low* (0.1)

$$\mathbf{LS} = \underbrace{LSA1 \times LSR1}_{\text{1st Opportunity}} + \underbrace{(1-LSA1)\, LSA2 \times LSR2}_{\text{2nd Opportunity}} + \underbrace{(1-LSA1)(1-LSA2)\, LSA3 \times LSR3}_{\text{3rd Opportunity}}$$

Where:

LSA = Likelihood of detection and correct alarm assessment, given an adversary attempt.

LSR = Likelihood of interception and neutralization, given detection and correct alarm assessment.

U.S. Department of Justice

(Reference 72, *Fiscal Year 1999 State Domestic Preparedness Support Program*)

Vulnerability Assessment Factors

1) Level of Visibility

Level of Visibility	Rating Value
Addresses the awareness of the existence and visibility of the target.	
Invisible - Classified Location	0
Very Low Visibility - Probably not aware of its existence	1
Low Visibility - Probably not well known existence	2
Medium Visibility - Existence is probably known	3
High Visibility - Existence well known	4
Very High Visibility - Existence is obvious	5

2) Criticality of Target Site to Jurisdiction

Criticality of Target Site	Rating Value
Usefulness of assets to population, economy, government, etc. Deemed critical to the continuity of basic jurisdiction infrastructure. (**Utilities, communications, water, gas, sewage, electrical, petroleum, transportation, medical facility, government facilities, hampers emergency response**)	
No Usefulness	0
Minor Usefulness	1
Moderate Usefulness	2
Significant Usefulness	3
Highly Useful	4
Critical	5

3) Value of Target to PTE

Value of Target	Rating Value
Evaluates value of the target to serve the ends of the PTEs identified in the Threat Assessment based on Motivations.	
None	0
Very Low	1
Low	2
Medium	3
High	4
Very High	5

4) PTE Access to Target

PTE Access to Target	Rating Value
Addresses the availability of the target for ingress and egress by a PTE.	
Fenced, Guarded, Protected Air/Consumable Entry, Controlled Access by Pass Only, No Vehicle Parking within 50 Feet	0
Guarded, Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Vehicle Parking within 50 Feet	1
Protected Air/Consumable Entry, Controlled Access of Visitors and Non-Staff Personnel, No Unauthorized Vehicle Parking within 50 Feet	2
Controlled Access of Visitors, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within 50 Feet	3
Open Access to all personnel, Unprotected Air/Consumable Entry, No Unauthorized Vehicle Parking within 50 Feet	4
Open Access to all personnel, Unprotected Air/Consumable Entry, Vehicle Parking within 50 feet	5

5) Target Threat of Hazard

Target Threat of Hazard	Rating Value
This assesses the presence of WMD Materials (BNICE) in quantities that would expend internal response capabilities if released.	
No WMD materials present	0
WMD materials present in moderate quantities, under positive control, and in secured locations.	1
WMD materials present in moderate quantities and controlled.	2
Major concentrations of WMD materials that have established control features and are secured in the site.	3
Major concentrations of WMD materials that have moderate control features.	4
Major concentrations of WMD materials that are accessible to Non-staff personnel.	5

6) Site Population Capacity

Site Population Capacity	Rating Value
Maximum number of individuals at a site at any given time.	
0	0
1 - 250	1
251 - 500	2
501 - 1000	3
1001 - 5000	4
> 5000	5

7) Potential for Collateral Mass Casualties

Potential for Collateral Mass Casualties	Rating Value
Addresses potential collateral mass casualties within a one-mile radius of the target site. Number ranges indicate inhabitants within a one-mile radius of the site.	
0 to 100	0
101 to 500	1
501 to 1000	2
1001 to 2000	3
2001 to 5000	4
> 5000	5

Individual Target Vulnerability Assessment Worksheet

Individual Target Vulnerability Assessment Values

Factor	Score
Visibility	
Criticality	
Value	
Access	
Threat of Hazard	
Site Population	
Collateral Mass Casualties	
	Total Score

Table 2-a-1

Individual Target Vulnerability Assessment Key

TOTAL SCORE	TARGET VULNERABILITY RATING
0-2	1
3-5	2
6-8	3
9-11	4
12-14	5
15-17	6
18-20	7
21-23	8
24-26	9
27-29	10
30-32	11
33-35	12

Consequence Assessment

Practice

New Mexico[21] and the Federal Aviation Administration[61] each use a consequence grid or matrix to determine the consequence of loss and are then assigned a numeric value. Generally, more than one aspect is considered in the measurement (ex: loss of life, economic impact, public outcry, etc.). The U.S. Coast Guard assigns categories of consequence a numeric/color value (1 low/green, 2-3 middle/yellow, 4-5 high/red).

New Mexico

(Reference 21, *Integrated Transportation Analysis Vulnerability Assessment: General Description*)

Figure 2, on page 6, illustrates three levels of consequence and three types of incidents. The types of incidents can be normal, abnormal or malevolent. Consequences can be low, medium or high and can relate to human life and economic impact.

The framework for ITA includes 5 elements:

- User
- Vehicle
- Infrastructure
- Social setting
- Environment

These elements are described on pages 7 and 8.

Federal Transit Administration

(Reference 64, *Transit Threat and Vulnerability Assessment Methodology*, p. 8)

Exhibit 3: Threat Impact Categories

Description	Category	Personnel	Service Disruption	Dollars Lost
Catastrophic	I	Loss of life	System Loss Long term (6 months or more) shutdown of line	Above $1M
Critical	II	Injury Serious occupational illness	Line loss for <6 months Loss of critical equipment	$250K to $1M
Marginal	III	Minor injuries or illness (no lost work days)	Line loss <1 hr. Car loss <5 days	Below $250K
Negligible	IV	No injury or illness	No service loss	No dollars lost

Federal Aviation Administration

(Reference 61, *Airport Vulnerability Assessment Methodology*, p. 3)

Consequence Scales

LEVEL OF CASUALTIES (F)		FACILITY I OWN TIME (U)		EXPOSURE (E)	
Very High (4)	>25 Fatalities	Very High (4)	>24 hours	Very High (5)	Public Outcry/ Dismay
High (3)	11-25 Fatalities	High (3)	>16 to 24 hours	High (4)	Congressional Mandates
Moderate (2)	1-10 Fatalities/ Multiple Injuries	Moderate (2)	>8 to 16 hours	Moderate (3)	Potential Litigation
Low (1)	1 Person Injured	Low (1)	8 hours or Less	Low (2)	Major Investigation
Very Low (0)	No Injuries	Very Low (0)	No Down Time	Very Low (1)	Minor Investigation

Countermeasures

Practice

Washington[52] documented specific retrofit techniques used to reinforce vulnerable bridges. Arkansas[1] and Texas[34] documented general security recommendations for each critical bridge (e.g., video surveillance, police presence, lighting, etc.). Maryland[19] documented current and desired security recommendations for the highest priority facilities.

State DOT

Bridges

- Video surveillance
- Fencing access area to operator
- Built-in monitors
- Increase lighting
- Motion devices below bridge
- Physical protection of piers
- Monitor river traffic
- Increase armed security
- Inspection of trucks
- Police presence: boat patrol
- Video coverage
- No-fly zone
- Courtesy patrols
- Video coverage under bridge

Tunnels

- Ventilation systems
- Video monitoring
- Building lock-down
- Checking truck traffic
- Enforcement of HAZMAT requirements
- Checking of driver credentials: truck inspection facility
- Application of X-ray technology
- Improved training for toll collectors and other personnel

Dams

- Visual inspection
- Truck station
- Increased lighting
- Addition of CCTV cameras

Cost Estimation

Practice

Most states do not document the costs of performing countermeasures. States that do provide documentation on costs only give a very general costing methodology.

Washington

(Reference 52, Bridge Seismic Retrofit pp. 18-20)

Superstructure Retrofit For Bridges (costs as of 1993)

- Concrete Box Girder — $1,050 per lineal foot of joint
- Concrete Flat Slab — $560 per lineal foot of joint
- Precast Concrete Beam — $375 per lineal foot of joint
- Steel Beam — $375 per lineal foot of joint
- Full height column w/footing — $1,000 per lineal foot of column
- Partial height column w/no footing height — $215 per lineal foot of column