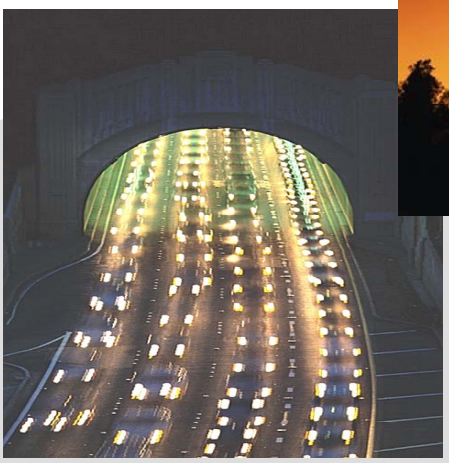
CONTRACTOR'S FINAL REPORT

A Guide to Highway Vulnerability Assessment

for Critical Asset Identification and Protection



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

Acknowledgements

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection ("Guide") is the result of the contributions from a number of individuals, agencies, and organizations. The National Cooperative Highway Research Program (NCHRP) funded the development of this Guide, and the Office of Engineering and Technical Services of the American Association of State Highway and Transportation Officials (AASHTO) sponsored its preparation. The AASHTO Task Force on Transportation Security served as the primary advisor for this Guide.

Much of the information contained in the Guide came from State Department of Transportation (DOT) representatives, and their contributions were critical in creating a document that reflects the needs of state and local transportation practitioners for conducting vulnerability assessments. Several federal agencies were also extremely helpful in providing information on the many subtleties of vulnerability assessment and critical infrastructure protection. In many cases, State DOTs have incorporated vulnerability assessment and critical infrastructure protection methods developed by federal agencies in their own programs, and several of these methods are among the preferred approaches presented in this Guide.

The preferred approaches to vulnerability assessment reflect the best judgment and experience of the employee-owners of Science Applications International Corporation (SAIC), who researched and developed this Guide. The principal investigator of the project was Dr. Michael C. Smith. The other primary authors of this Guide are Dr. Shahed Rowshan, Stephen J. Krill, Jr., Jennifer E. Seplow and William C. Sauntry. David J. Hensing served as a senior reviewer along with many State DOT representatives whose comments greatly improved the Guide. The contents of this Guide were derived from personal interviews, literature reviews, and previous work in this area, but they do not represent an official view of any sponsor, State DOT, or federal agency.

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.

DISCLAIMER

This is an uncorrected draft as submitted by the research agency. The opinions and conclusions expressed or implied in the report are those of the research agency. They are not necessarily those of the Transportation Research Board, the National Research Council, the Federal Highway Administration, the American Association of State Highway and Transportation Officials, or the individual states participating in the National Cooperative Highway Research Program.

Executive Summary

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection ("Guide") was prepared under the direction of the National Cooperative Highway Research Program (NCHRP) for the American Association of State Highway and Transportation Officials (AASHTO) to address our nation's vulnerability assessment needs for highway transportation subsequent to the terrorist attacks of September 11th, 2001.

This Guide was developed as a tool for State Departments of Transportation (DOTs) to:

- Assess the vulnerabilities of their physical assets such as bridges, tunnels, roadways, and inspection and traffic operation facilities, among others;
- Develop possible countermeasures to deter, detect, and delay the consequences of terrorist threats to such assets;
- Estimate the capital and operating costs of such countermeasures; and
- Improve security operational planning for better protection against future acts of terrorism.

This Guide can benefit a broad audience in the State DOTs, including senior officials involved in the initial planning stage of the vulnerability assessment process, mid-level managers charged with developing the assessment plans and procedures, and field personnel who will likely conduct the assessments of critical assets. The Guide recommends that State DOTs organize and manage a multidisciplinary team whose members must possess a working knowledge of the department's mission, its critical assets, and its policies, plans and procedures. The Guide also identifies the types of resources typically required by the team to conduct a vulnerability assessment, and it describes the three major phases of the process – pre-assessment, assessment, and post-assessment.

The vulnerability assessment process presented in this Guide is derived from a careful review of information compiled from state, federal, and international agencies and their personnel. The Guide provides six steps for conducting a vulnerability assessment of highway transportation assets. These six steps provide a straightforward method for examining critical assets and identifying cost-effective countermeasures to guard against terrorism. For each step, the objective is clearly stated, the practice of that step by other state and federal agencies is referenced, a detailed approach is described, and illustrative examples are provided. The majority of examples provided in the Guide are based on actual applications by state and federal agencies. The criteria used in selecting the preferred approaches include availability, accessibility, transparency, replicability, reasonableness, scalability, robustness, cost-effectiveness, and modularity.

The Guide describes general methods that apply to a wide range of asset types. The vulnerability assessment methods in this Guide are applicable to any State DOT,

regardless of the extent, if any, of its critical infrastructure protection program. For states just starting this process, the Guide will provide a roadmap of issues to consider and actions to take during each phase of the vulnerability assessment – pre-assessment, assessment, and post-assessment. For states that have already begun this process, the Guide may provide alternate methods used by other states and federal agencies that could help to validate the work performed to date.

Table of Contents

Acknowledgements I

Executive Summary II

Table of Contents IV

Tables and Figures V

Introduction 1
Purpose of this Guide 1
Benefits from using this Guide 2
Target Audience for this Guide 2
Scope of this Guide 3
Assumptions 3
How to use this Guide 4

Vulnerability Assessment Overview 5
General Approach 5
Team Composition 5
Required Resources and Level of Commitment 7

Step 1 – Critical Assets Identification 9
Objective 9
Approach 9
Illustrative Example 13

Step 2 – Vulnerability Assessment 15
Objective 15
Approach 15
Illustrative Example 20

Step 3 – Consequence Assessment 21
Objective 21
Approach 21
Illustrative Example 22

Step 4 -- Countermeasures 25
Objective 25
Approach 25
Illustrative Example 28

Step 5 – Cost Estimation 29
Objective 29

Approach 29
Illustrative Example 31

Step 6 – Security Operational Planning 33
Objective 33
Approach 33

Appendix 38

Vulnerability Assessment Guide Comments 39

Tables and Figures

Table 1 - Critical Transportation Assets 10

Table 2 - Critical Asset Factors and Values 12

Table 3 - Critical Asset Scoring 13

Table 4 – Example Scoring Table for Identifying and Prioritizing Critical Assets 14

Table 5 - Vulnerability Factor Definitions 17

Table 6 - Vulnerability Factor 18

Table 7 – Vulnerability Factor Default Values and Definitions 18

Table 8 - Vulnerability Factor Scoring 19

Table 9 – Example Scoring Table for Assessing Vulnerabilities 20

Table 10 – Example Criticality and Vulnerability Coordinates and Related Quadrants 23

Table 11 - Potential Countermeasures 26

Table 12 – Illustrated Example – Applying Countermeasures to Critical Asset Categories 28

Table 13 – Countermeasure Relative Cost Range 30

Table 14 - Estimated Countermeasure Costs 30

Table 15 – Illustrative Example of Countermeasure Costs 31

Figure 1 – Six Steps for Conducting a Highway Vulnerability Assessment 5

Figure 2 – Staffing the Vulnerability Assessment Process 6

Figure 3 – Typical Vulnerability Assessment Schedule 8

Figure 4 – Homeland Security Advisory System 16

Figure 5 – Criticality and Vulnerability Matrix 22

Figure 6 – Illustrative Example of Criticality and Vulnerability Matrix 23

Introduction

The consequences of a terrorist attack against the nation's highway infrastructure could result in multiple injuries and fatalities, the disruption of vehicular traffic and commerce, and significant regional or national economic losses. Specific assets within this infrastructure may also be at risk simply because of their symbolic nature or potential use as a launching pad for weapons of mass destruction.

A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection ("Guide") was developed under the direction of the National Cooperative Highway Research Program (NCHRP) for the American Association of State Highway and Transportation Officials (AASHTO) as a companion to the Guide to Updating Highway Emergency Response Plans for Terrorist Incidents.[1] These two documents were prepared as part of the AASHTO Task Force on Transportation Security's action plan for addressing our nation's transportation security needs in the aftermath of the terrorist attacks of September 11th, 2001. The Guide is designed to assist State Departments of Transportation (DOTs) in assessing the vulnerability of their highway transportation assets. The companion guide, prepared in parallel with this Guide, assists State DOTs in preparing and executing a coordinated emergency response to terrorist threats or attacks to the highway transportation system. The intent of the AASHTO Task Force in both of these action items was to discover what is currently being done or is under development in selected states and to provide "best practices" in the form of a guide or handbook that State DOTs may use to prepare for and respond to future acts of terrorism.

This Guide provides a starting point to help State DOTs identify and mitigate the vulnerabilities of and consequences to highway transportation assets from terrorist threats or attacks. As more states gain experience in highway vulnerability assessment and as our nation gains a better understanding of terrorist threats to our critical infrastructure, the Guide can be updated, expanded, and refined to reflect this additional level of understanding and experience.

Purpose of this Guide

The Guide was developed as a tool for State DOTs to:

- 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,
- Estimate the capital and operating costs of such countermeasures, and
- Improve security operational planning for better protection against future acts of terrorism.

[1] The *Guide to Updating Highway Emergency Response Plans for Terrorist Incidents* was prepared by Parsons Brinkerhoff for AASHTO in parallel to the development of this vulnerability assessment guide.

This Guide is based primarily on "best practices" identified in states that have begun the process of assessing the vulnerability of their highway transportation infrastructure, as well as similar methods from other relevant sources.

Benefits from using this Guide

The Guide describes general methods that apply to a wide range of asset types. The vulnerability assessment methods in this Guide are applicable to any State DOT, regardless of the extent, if any, of its critical infrastructure protection program. For states just starting this process, the Guide will provide a roadmap of issues to consider and actions to take during each phase of the vulnerability assessment – pre-assessment, assessment, and post-assessment. For states that have already begun this process, the Guide may provide alternate methods used by other states and federal agencies that could help to validate the work performed to date.

Some of the specific benefits of applying the approaches presented in this Guide include:

- Enables elected and appointed officials to set priorities commensurate with the degree of risk facing highway transportation assets,
- Provides descriptive information on each potential asset in the state,
- Establishes a methodology for comparison of both similar and vastly different types of assets,
- Justifies management decisions for altering programming, budgeting, and staffing assignments that may differ from previous norms,
- Encourages identification of technical and research needs in asset protection and emergency management,
- Provides tools to raise the level of understanding of public officials and to influence the adoption of mitigation measures and expenditures of resources to do so,
- Enables the establishment of a viable geographic information system database of asset criticality and vulnerability and other relevant comparable information for planning,
- Remains flexible enough to accommodate assessments that were done in the past as well as those to come in the future, and
- Allows for the information to be used in other similar assessments (i.e., natural and technological disasters).[2]

Target Audience for this Guide

This Guide was developed for State DOT personnel involved with the planning, review, and execution of highway vulnerability assessments. The audience includes senior officials involved in the initial planning stage of the vulnerability assessment process, mid-level managers charged with developing the assessment plans and

[2] From Iowa's Homeland Security Critical Asset Assessment Model (CAAM) (Reference 16).

procedures, and field personnel who will likely conduct the assessments of critical assets.

The users of this Guide need not be proficient in vulnerability assessment, however, they need a strong working knowledge of the department's mission, its critical assets, and its policies, plans and procedures in order to implement this process. The Guide provides sufficient background so that other DOT managers and operations personnel can understand its intent and context.

Scope of this Guide

Vulnerabilities in highway transportation generally fall into three categories:

(1) The physical facilities themselves,

(2) The vehicles (private and commercial motor carriers) operating on the system, and

(3) The information infrastructure that monitors and manages the flow of goods, vehicles, and people on the highway system.

This Guide deals with physical highway transportation assets such as bridges, tunnels, roadways, interchanges, tollhouses, and roadside infrastructure (e.g., signs, barriers, sensors), among others.

Assumptions

Vulnerability assessment methods range in complexity from highly subjective approaches that rely primarily on the good judgment of knowledgeable and experienced individuals to detailed scientific approaches involving structural analyses and testing. Historically, vulnerability assessments related to highways have focused on natural and unintentional technological disasters where reasonable estimates of destructive forces can be estimated and engineering designs can be developed consistent with perceived risks to critical infrastructure, people and property.

Terrorism presents an "asymmetric" threat – one in which terrorists employ surprise and relatively low-cost weaponry to inflict catastrophic damage on large populations and property, instilling fear and panic or threaten to do so, causing similar disruption or panic. Vulnerability to these threats is much more difficult to assess and is often based on assumptions about the capability and intent of terrorist organizations. The best countermeasures may involve access control, surveillance, monitoring, standoff barriers, and other procedural or technical approaches rather than improving structural integrity of the asset itself through engineering design and construction.

With this in mind, users of this Guide are assumed to have sufficient knowledge (or have access to those that do) of real or potential threats to highway-related physical assets and to be capable of making the judgments required in the preferred approaches contained in this Guide. In general, the approaches for each of the steps provided in this Guide help users divide the assessment into components where

informed judgments can be made and then "rolled-up" to form an ordered list of assets, threats, and countermeasures that will inform decision-makers concerning investments in specific vulnerability reduction strategies.

How to use this Guide

Use of this Guide depends on the status of vulnerability assessment in each state. Based on the states interviewed, some states have not begun the vulnerability assessment process while others already have a method in place and are using it to assess critical infrastructure.

Prior to using the Guide, the user must understand that the Guide offers a general method that applies to all forms of highway infrastructure. As critical assets differ nationally, each State DOT may follow the steps in the approach somewhat differently. For instance, some states may have no tunnels, so any aspect of the approach that relates to tunnels can be eliminated for those states. To highlight this concept, text boxes have been placed within the Guide to illustrate the differences in states' assessment results.

States that do not currently have a vulnerability assessment (VA) plan should use this Guide in its entirety to complete their first critical highway infrastructure vulnerability assessment. From this initial assessment, they should gain an understanding of what aspects of the Guide best apply to their infrastructure and then use this understanding to complete future assessments. Each state may use the approach differently as they become more familiar with the process. Most importantly, states should continue to assess the approach as it applies to their assets to ensure that they are obtaining the most complete results.

For states that do have a VA plan in place, this Guide provides an opportunity to assess and validate existing methods. As several states have VA plans that were prepared prior to September 11th, this Guide can be used as a basis for updating those plans. States can complete a vulnerability assessment using the steps provided in the Guide to determine if their current approach provides similar results. This comparison can be used to either validate the current approach or to determine that the approach should be augmented by or completely replaced with the approaches suggested in the Guide.

Vulnerability Assessment Overview

General Approach

Figure 1 displays the six steps for conducting a vulnerability assessment of highway transportation assets.

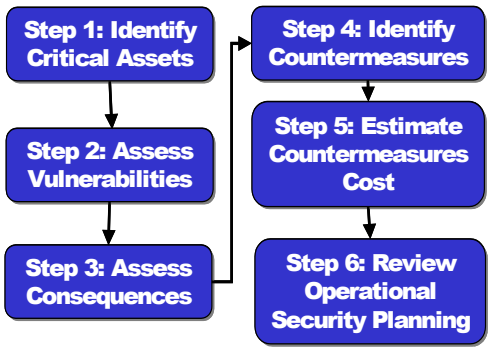


Figure 1 – Six Steps for Conducting a Vulnerability Assessment

As illustrated, these six steps represent an integrated and iterative approach to vulnerability assessment. This approach depends upon the formation of a dedicated, multidisciplinary team with ready access to a range of resources – from databases to personnel – as well as a commitment from senior State DOT officials to examine critical assets carefully and identify cost-effective countermeasures to provide better protection against the threats of terrorism involving the use of weapons of mass destruction (WMD).

Team Composition

This Guide assumes that the State DOT will organize a multidisciplinary team whose members possess a working knowledge of the department's mission, critical assets, and policies, plans and procedures. Team members should represent important departmental functions such as:

- Budget
- Environmental management
- Maintenance
- Purchasing
- Construction
- Facilities management
- Materials testing
- Safety
- Design
- Human resources
- Planning
- Traffic operations
- Communications

Given that the information on threats, vulnerabilities and consequences will probably come from sources external to the State DOT, the team will need to either include or frequently interact with other state and local organizations representing law enforcement, fire services, public safety, public health, and emergency management. Interaction with these sources must occur early on in the assessment and continue throughout to ensure proper coordination and cooperation.

As the team will be composed of representatives from different State DOT departments as well as from external organizations, team members will likely have differing knowledge and different ways of working. Furthermore, as most State DOTs have had little experience in dealing with terrorism, many of the concepts used

in the assessment may be unfamiliar. To address these issues and ensure that the team is well prepared to complete the assessment, training exercises should be held prior to beginning the vulnerability assessment. These exercises should include classroom style sessions and tabletop exercises. The classroom sessions should give instruction on the importance of the assessment, establish a common set of assumptions, and give an overview of the steps for completing the assessment as well as what is to be done post-assessment. The tabletop exercises should simulate an actual vulnerability assessment, giving team members a chance to work through each of the steps and ask questions before they begin the actual assessment.

A team leader should be selected whose responsibilities include:

- Providing technical direction and management of the team members,
- Maintaining overall responsibility for team performance,
- Ensuring access to technical and managerial resources,
- Initiating quality control on all team activities,
- Developing and monitoring schedule and cost control, and
- Maintaining communications with senior management.

The composition of the team, the number of members assigned, and the level of experience and training will have a direct effect on the outcome and timetable of the vulnerability assessment. The multidisciplinary team will be responsible for selecting and assigning values to important factors in the steps outlined in this Guide that determine the prioritization of the critical assets and identification of the most vulnerable assets.

Figure 2 illustrates how the team works through the vulnerability assessment process to evaluate critical assets. Note that different skills, knowledge, and experience may be required for different aspects of the vulnerability assessment. *Transportation professional* in State DOTs and local Departments of Public Works (DPWs)

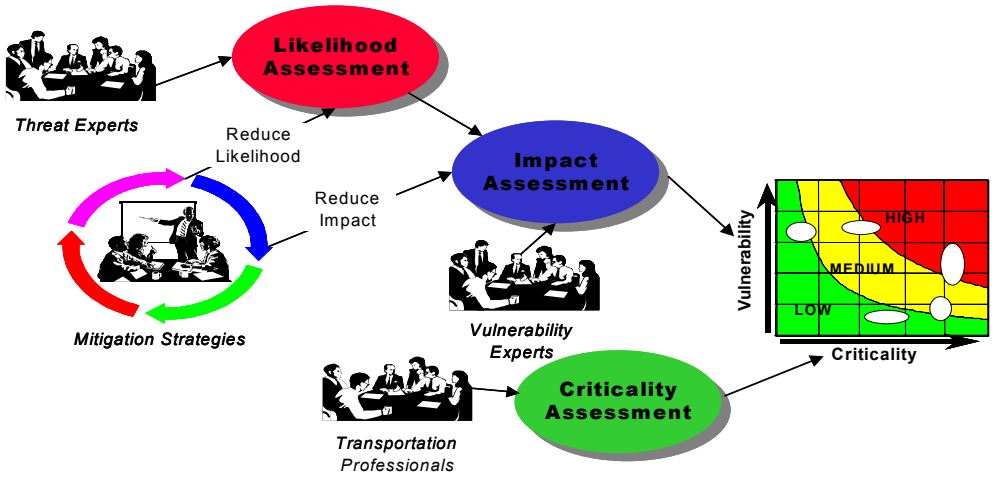


Figure 2 – Staffing the Vulnerability Assessment Process

understand mobility, transportation operations, and structural design issues. *Threat experts* typically reside in federal, state, and local law enforcement agencies; *vulnerability experts* may be design engineers, security specialists, or operating personnel familiar with control procedures and operating parameters. Personnel involved in developing *mitigation strategies* may be law enforcement personnel, technology vendors, engineers, security specialists, site managers, resource specialists and others who might suggest options for reducing the likelihood of attack or the impact if an attack should occur.

Required Resources and Level of Commitment

Support from senior management is paramount to the team's success, especially as it affects the team's access to a variety of resources throughout the department, and in some cases throughout the state government. The following list identifies the types of resources typically required by the team to conduct a highway vulnerability assessment. Whenever possible, specific data sources are identified to help the team collect the information needed to conduct the assessment.

- Asset data
  - National Bridge Inventory System
  - Hazardous Materials Information System
- Threat data
  - Law Enforcement
  - State's Emergency Management Agency
  - Homeland Security Office
- Vulnerability data
- Consequence data
- Countermeasures data
- Cost data
- Policies, plans, and procedures
- Personnel (interviews)
- Geographic information systems (maps, drawings)

Time is one of the most important resources available to the team. The vulnerability assessment process typically occurs in three major phases: (1) pre-assessment, (2) assessment, and (3) post-assessment. The entire process may take as much as six months of dedicated staff time to collect and assess the data and to validate and implement the results. Within this time period it may be difficult for team members to carry out normal job functions while working on the vulnerability assessment. This should be noted when planning for the assessment and the appropriate staffing reassignments should be made prior to beginning the assessment.

- In the first phase (pre-assessment), the department assembles the assessment team, conducts team training exercises, makes contact with external organizations, plans and schedules the vulnerability assessment process, and collects the required resources.

- In the second phase (assessment), the team conducts the vulnerability assessment by making use of available data sources, physically examining critical assets, interviewing personnel, assessing the data, and making recommendations on countermeasures.

- In the third phase (post-assessment), the department, working with the team, develops a strategy for implementing the recommended countermeasures. Activities in this phase may include conducting cost-benefit analyses and trade-off studies and procuring equipment and services. The Guide encourages immediate procurement action, as the assessment serves no purpose without actually installing the proper countermeasure equipment and services.

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

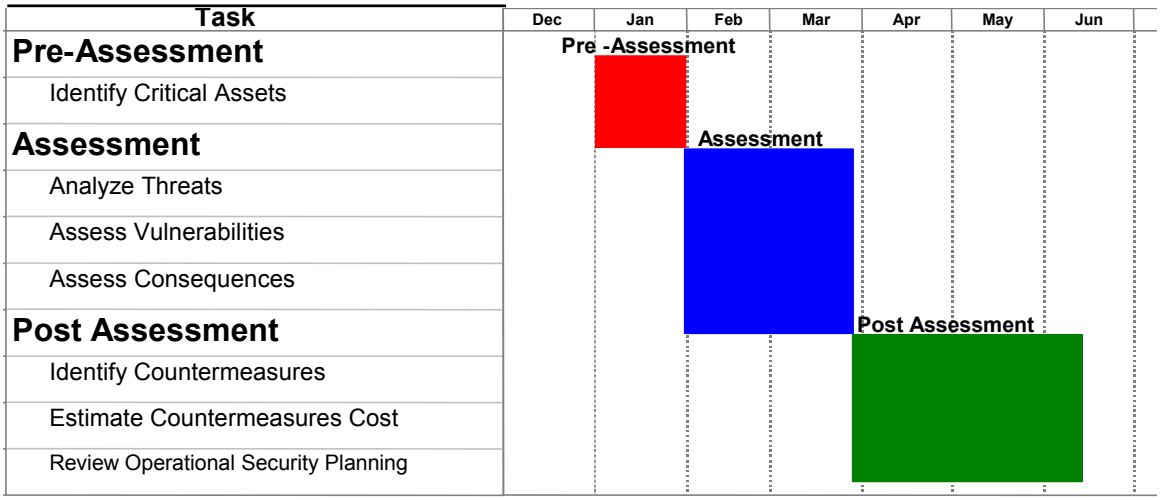


Figure 3 – Typical Vulnerability Assessment Schedule

Lastly, this process produces an integrated report, consolidating the information obtained while conducting the vulnerability assessment. At a minimum, the report should include:

- Assessment of identified critical assets,
- Analysis of the threats to and vulnerabilities of those assets,
- Analysis of the consequences of the threats to and vulnerabilities of those assets,
- Recommendations to reduce vulnerabilities and mitigate consequences by means of countermeasures, and
- Other information essential for the development of operational security plans to mitigate the consequences.

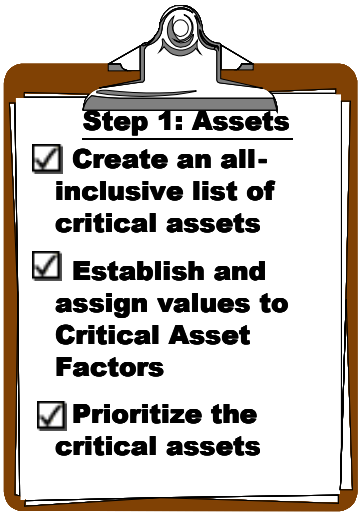
CAUTION!

The methodology in this Guide is an iterative process. The State DOTs are encouraged to review the Guide in its entirety prior to beginning the implementation. Areas that require early planning include budgeting for the cost of countermeasure procurement and initiating training including tabletop exercise activities.

Step 1 – Critical Assets Identification

Objective

The objective of Step 1 is to identify those assets – infrastructure, facilities, equipment, and personnel – deemed "critical" for achieving the department's primary mission.



Approach

State DOT officials may use the following three-step approach to either validate an existing list or develop an initial list of critical assets.

☑ 1a – Create an all-inclusive list of critical assets

Identification of critical assets begins with organizing a team of experienced staff most familiar with the highway assets of the state. This team could include a number of members from the overall assessment team such as operations and maintenance staff, design and construction engineers, traffic engineers, and field personnel. One approach is for the team to start the process by reviewing the department's mission and answering the following question:

"Which assets enable us to achieve our mission?"

Considering the mission statement and their knowledge of the state's critical highway assets, the team could begin with organizing transportation assets into the following four categories:

- Infrastructure
- Facilities
- Equipment
- Personnel

The table below provides examples of critical transportation assets based upon information collected in the survey of State DOTs. However, note that the focus of this Guide is highway related 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.

Example: Utah's Critical Assets

The Utah Department of Transportation (UDOT) identified the following types of assets as critical for meeting its mission statement in preparation for hosting the 2002 Olympic Winter Games in Salt Lake City:

- Facilities: Infrastructure – highways, bridges, tunnels, and roadways upon dams; buildings – UDOT headquarters, traffic operations center, regional complexes (3), maintenance stations (18), and ports of entry (3)

- Equipment: Vehicles – snow removal, maintenance, and incident management; Variable Messaging System; hazardous materials, including ammunition (for avalanche control)

- Personnel: UDOT employees; contractors; vendors

Example: Maryland's Critical Assets

Maryland developed a list of potential targets grouped into the following twelve categories:

1. Bridges & Overpasses
2. Major Office Complexes
3. Communications Control Points
4. Interstate Roads
5. Arterial Roads
6. Maintenance Facilities
7. Regional Laboratories
8. District Office Buildings
9. Satellite Maintenance Facilities
10. Magnesium Chloride Storage
11. Salt Storage
12. Rest Areas

☑ 1b – Establish and assign values to the critical asset factors

Critical asset factors are the criteria used to identify and prioritize critical assets. Collectively, these factors are an indication of the conditions, concerns, consequences, and capabilities that might cause a State DOT to label an asset "critical." Each factor is assigned a value based on the importance of the factor in establishing an asset as "critical." The factors and associated values shown in Table 2 serve as a guide for scoring and ranking the all-inclusive list of critical assets.

The sample values listed in Table 2 are derived primarily from work done in the State of Texas (reference 35), augmented by factors derived from the work of other states and federal agencies. State DOTs may choose to use this list as it is or they can adjust and augment the list based on their particular needs. However, prior to beginning the assessment, the review team should agree on the list of factors and their individual values. Once the factors and values have been determined, this list must remain constant throughout the entire assessment. In fact, if the factor values and asset scores are not carefully examined for uniformity and consistency, multiple teams assigning Critical Asset Factors and scores could result in inconsistencies in the prioritization of critical assets. If, after beginning the assessment process, the team adjusts the critical asset factors or their respective values, the team may need to reassess some assets to ensure consistency.

The factor values assigned are based on the importance of the factor in labeling the asset as critical. The values assigned to factors range from "extremely important" (5)

to "less important " (1). Note that the assignment of these factor values to assets is binary. If the critical asset factor applies to the asset being evaluated, then the asset receives the value assigned to that factor. However, if the factor does not apply, the asset is assigned a value of 0 for that factor. Some states may choose to have two or more similar factors that distinguish between different levels. For example, if a state chooses to distinguish between "medium" and "major" economic impact, the team might assign the factor "Medium Economic Impact" a value of "3" and the factor "Major Economic Impact" a value of "5." Note, however, that every asset is assessed for every factor so adding more factors increases the number of judgments required.

Table 2 lists the critical asset factors, their values and a description for each factor. Note that the factors are grouped into categories of related factors.

Table 2 - Critical Asset Factors and Values

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?

☑ 1c – Prioritize the all-inclusive list of critical assets

In this step, the assessment team assigns priorities to critical assets. The letters A through N in Table 3 correspond with the critical asset factors listed in Table 2. For each asset, the applicable critical asset factor values are entered. The sum of these values (x) represents the total score for that asset. These scores are ordered from highest to lowest. The total score for the most critical assets are used in Step 3. The maximum possible criticality value (C_{max}), based on the values used in Table 2, is 43. C_{max} for each agency will vary based on the values assigned to Critical Asset factors in Table 2.

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

CAUTION!

At this point in the vulnerability assessment process, the number of assets deemed critical should be carefully examined. The more assets remaining on the list, the more time and resources needed to complete the assessment. The first focus should be on the assets deemed most critical to the agency's mission.

Illustrative Example

The following hypothetical example illustrates the results from Step 1. In this example, the State DOT elected to exclude from assessment those critical assets from the equipment and personnel categories.

Table 4 – Example Scoring Table for Identifying and Prioritizing Critical Assets

CRITICAL ASSET	CRITICAL ASSET FACTOR														TOTAL SCORE (x)
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	1	*2*	*5*	*1*	*3*	*3*	*5*	*5*	*5*	*4*	*1*	*5*	*2*	*1*	
Smith Bridge	1	2	5	1	3	3	5	5	5	4	1	5	2	1	43
Bayside Tunnel	1	2	5	1	3	3	5	5	5	4	1	5	2	1	43
Blue Bridge	1	0	5	0	3	3	5	5	5	4	0	5	2	0	38
Crystal Bridge	1	2	5	1	3	3	0	5	5	0	0	5	2	1	33
Interstate 1	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Interstate 218	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Interstate 88	1	2	5	1	3	3	5	0	0	4	1	5	2	1	33
Rt. 49	1	2	5	0	3	3	5	0	0	4	1	5	0	1	30
Rt. 6	1	2	5	0	3	3	5	0	0	4	1	5	0	1	30
Johnson Interchange	1	0	5	0	3	3	5	0	0	4	0	5	2	0	28
Headquarters Building	1	2	0	1	3	3	0	0	0	0	1	0	2	1	14

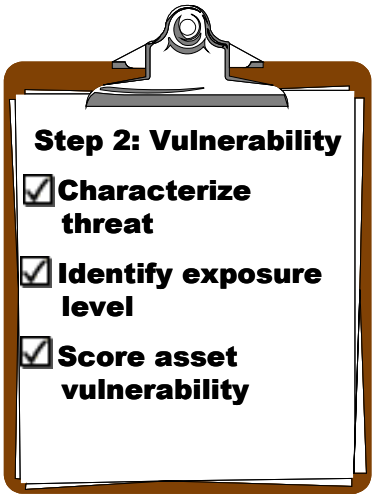
After calculating the scores and ranking the critical assets, a screening threshold is applied, such as "top ten percent (10%)," to eliminate low-scoring assets.[3] The assessment team sets the threshold based on their experience, familiarity with the assets, and the needs of the state. The selected items form the prioritized critical asset list, which will be assessed to determine threats, vulnerabilities, consequences, and countermeasures.

[3] This value is consistent with the U.S. Department of Justice (USDOJ) Needs Assessment Program.

Step 2 – Vulnerability Assessment

Objective

The vulnerability assessment is designed to systematically identify and evaluate critical assets in terms of their susceptibility to and the consequences of terrorist attacks. The process described below identifies exposures and weaknesses that can be exploited by terrorists.



Approach

☑ 2a – Characterize the threat

This step is particularly challenging for State DOTs because, while the vulnerability assessment will typically be done periodically (e.g., annually or bi-annually), the threat is dynamic and clouded with uncertainty. Consequently, threat characterization for the purposes of vulnerability assessment is different from what might be used on a day-to-day basis as part of an operational security plan (see Step 6).

The U.S. Department of Justice (USDOJ) developed an approach for threat analysis as part of its "State Domestic Preparedness Equipment Program." This approach is used to assess the capabilities and needs of first responders for acts of WMD terrorism. Working closely with other federal agencies, USDOJ is engaging city, county, and state fire services, hazardous materials, law enforcement, public works, emergency management and public health officials to help individual jurisdictions pinpoint vulnerabilities and develop plans for countering WMD terrorism. The national assessment results serve as both a roadmap for program planning and a benchmark for measuring program effectiveness.

As part of its responsibilities under the "State Domestic Preparedness Equipment Program," each state and Territory will use the findings from the assessments as the basis for developing a domestic preparedness strategy for allocating first responder training, technical assistance and exercise support resources. During the last year, states and Territories conducted an integrated vulnerability, threat, and public health assessment that considered facilities, sites, systems, and/or special events within their jurisdiction. These assessments included facilities, sites, systems, and/or special events involving transportation.

A few states have adopted this threat analysis approach from the "State Domestic Preparedness Equipment Program." Still, USDOJ presents the following disclaimer about threat analysis:

> *"Although threat information is deemed beneficial to the [assessment], it should not be given undue weight. There remains insufficient empirical data on*

domestic terrorist activity to suggest a pattern of particular targeting of a specific region or city. Henceforth, it must be recognized that the identification of a particular threat is not an absolute predictor that a terrorist incident will occur."

Recently the Bush Administration established the "Homeland Security Advisory System" to improve coordination and communication among all levels of government and the American public in the fight against terrorism.[4] This system provides a national framework for communicating the nature and degree of terrorist threats between government officials and the citizens they represent. At this time, the system uses a variety of factors to assess the threat, such as:

Figure 4 – Homeland Security Advisory System

- Is the threat credible?
- Is the threat corroborated?
- Is the threat specific and/or imminent?
- How grave is the threat?

Given the dynamic nature and the level of uncertainty of the threat, most State DOTs will find that the most effective approach is to consider the following criteria and make an informed judgment as to whether any or all of these factors apply with respect to transportation assets of interest:

- *Existence* – Is there a group or individual that is known to or potentially could be operating within the jurisdiction with the capability to create and/or to use a WMD?
- *History* – Has the jurisdiction experienced any past terrorist activity?
- *Intent* – Are there credible advocacy/threats of force or violence, or acts, or preparations to act, evidencing the intent to create a WMD or to use a WMD?
- *Capability* – Is there credible information that a specific group or individual possesses the needed training, skills, finances, and access to resources to develop or acquire a WMD?
- *Target* – Is there credible information indicative of preparations for specific terrorist operations against a critical asset?

A "yes" to any one of these questions is sufficient to raise concerns about threats to transportation assets in the state. A "yes" to the last question is indicative of an imminent threat. Obviously, the answers to these questions can change over time, thus the State DOT is well advised to plan conservatively for critical assets (i.e.,

[4] Source: White House Office of the Press Secretary. Governor Ridge Announces Homeland Security Advisory System. 12 March 2002. Found on the Internet at http://www.whitehouse.gov/news/releases/2002/03/20020312-1.html (Reference 73).

assume a credible threat exists), even though no solid intelligence or law enforcement agency information may be available to substantiate the assumption.

With this in mind, the next sub-steps in the vulnerability analysis should be based on assumptions about the real or potential intent and capability of the threat. This includes assumptions about the value the threat may place on certain assets for political or morale purposes, the threat's ability to gain access to critical assets, and the disruptive or destructive capability of the weapons the threat may employ (including threatening statements, hoaxes, and real weapons of mass destruction).

This Guide does not offer a specific quantitative technique for characterizing the threat (although the DOJ approach is available for states that wish to use it). Rather, State DOTs are encouraged to consider in broad terms the types of threats they seek to address and proceed with the vulnerability assessment accordingly.

☑ 2b – Assign vulnerability factors to the critical assets

This Guide uses the following vulnerability factors to analyze the potential vulnerabilities of critical assets:

Table 5 - Vulnerability Factor Definitions

VULNERABILITY FACTOR	***DEFINITION***
Visibility and Attendance	Awareness of the existence of the asset and the number of people typically present
Access to the Asset	The availability of an asset to ingress and egress by a potential threat element
Site Specific Hazards	The presence of materials that have biological, nuclear, incendiary, chemical, or explosive properties in quantities that would expend initial response capabilities if compromised

The vulnerability factors are comprised of two sub-elements each. These sub-elements will be used to calculate the vulnerability factor in the next section.

Table 6 - Vulnerability Factor Sub-Elements

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)

For the sub-elements shown in Table 6, values ranging from "extremely important" (5) to "less important" (1) are assigned. Table 7 indicates typical values assigned for the vulnerability factor sub-elements. Note that the scores assigned to critical assets should reflect judgments made based on analysis regarding the existence and capabilities of real or potential threats to the assets as discussed in sub-step 2a above.

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

VULNERABILITY FACTOR and DEFAULT VALUE			DEFINITION
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

In the above table, under Security Level (D), protected access is defined as structural and/or electronic security measures such as fencing, alarms, cameras, or locks. Controlled access is defined as entry validated by personnel such as armed or unarmed guards. Response force is where personnel are available to respond to either protected or controlled access violations.

☑ 2c – Score the vulnerability factor for each critical asset

In this step, the following formula is used to calculate the vulnerability factor (y) for each critical asset. In the formula, the sub-elements are multiplied by each other for visibility and attendance (A * B), for access to the asset (C * D), and for site specific hazards (E * F). The three resulting numbers are then added.

$$\text{Vulnerability Factor (y)} = (A * B) + (C * D) + (E * F)$$

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:

$$\text{Vulnerability Coordinate (Y)} = (y/75) * 100$$

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												

After calculating a total score for each critical asset, the scores are prioritized from highest to lowest.

Illustrative Example

The following hypothetical example illustrates the results from Step 2.

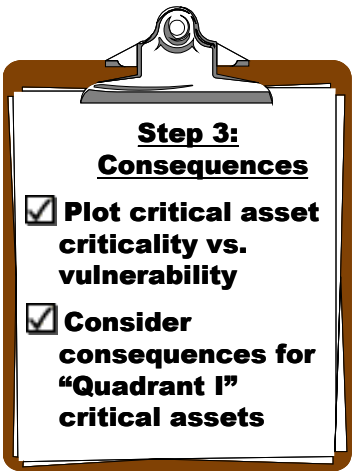
Table 9 – Example Scoring Table for Assessing Vulnerabilities

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	
Smith Bridge	5		2		5		5		4		2	43
Bayside Tunnel	4		5		4		3		3		2	38
Blue Bridge	3		4		3		5		5		3	42
Crystal Bridge	2		3		4		3		2		4	26
Interstate 1	4		2		3		4		4		5	40
Interstate 218	3		3		4		4		2		4	33
Interstate 88	4		4		3		3		4		5	45
Rt. 49	5		5		1		3		5		2	38
Rt. 6	3		3		3		4		5		3	36
Johnson Interchange	2		4		2		4		1		4	20
Headquarters Building	5		5		1		5		3		2	36

Step 3 – Consequence Assessment

Objective

The consequence assessment helps identify assets which, if attacked, produce the greatest risks for undesirable outcomes given a specific set of circumstances and conditions. This assessment is based on an integrated analysis of the data collected on critical/key assets/activities, realistic and credible threats, and known or specifically identified vulnerabilities.



Approach

☑ 3a – Plot critical asset criticality versus vulnerability

In this step, criticality (X) and vulnerability (Y) coordinates are calculated for each asset. The X and Y coordinates define a point for each asset in one of the four quadrants in the Criticality and Vulnerability Matrix of Figure 5. The criticality coordinate (X) is calculated based on the procedure described in Step 1 (Table 3). The vulnerability coordinate is calculated based on the procedure described in Step 2 (Table 8). X and Y coordinates plot the criticality and vulnerability for each critical asset:

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

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

where x and y are the raw values of criticality and vulnerability for each asset and C_{max} is the maximum possible Criticality value (C_{max}= 43 for the default values given in Step 1)

Figure 5 - Criticality and Vulnerability Matrix

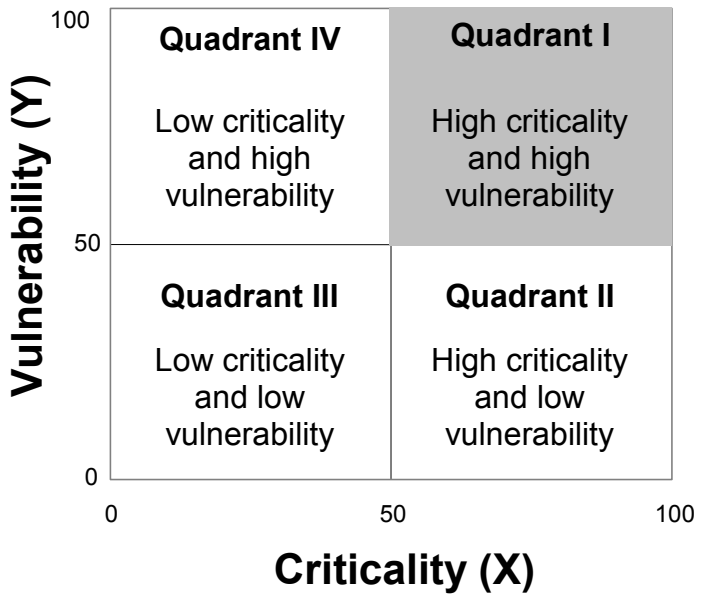


Figure 5 helps prioritize critical assets by the greatest level of consequence based on the critical asset factors and vulnerabilities evaluated previously. Quadrant I identifies the assets with the highest criticality and vulnerability for implementing countermeasures.

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.

Table 10 – Example Criticality and Vulnerability Coordinates and Related Quadrants

CRITICAL ASSET	CRITICALITY		VULNERABILITY		QUADRANT
	(x)	(X)	(y)	(Y)	
Smith Bridge	43	100	43	57	I
Bayside Tunnel	43	100	38	51	I
Blue Bridge	38	88	42	56	I
Crystal Bridge	33	77	26	35	II
Interstate 1	33	77	40	53	I
Interstate 218	33	77	33	44	II
Interstate 88	33	77	45	60	I
Rt. 49	30	70	38	51	I
Rt. 6	30	70	36	48	II
Johnson Interchange	28	65	20	27	II
Headquarters Building	14	33	36	48	III

Figure 6 shows the scatter diagram for the criticality and vulnerability coordinate values shown in the illustrative example. Note that, for this example, the Quadrant I assets include bridges, tunnels, and major interchanges. Each State DOT will find that the assets that fall in Quadrant I reflect the perceived vulnerabilities and characteristics of the asset (as captured on the vulnerability assessment) and the importance of the asset to the region (in terms of the critical asset factors). Also, note that some assets are critical to the state or region but judged to be less vulnerable, possibly due to redundant facilities, minimal consequences, or their physical characteristics that make them less susceptible to terrorist attacks.

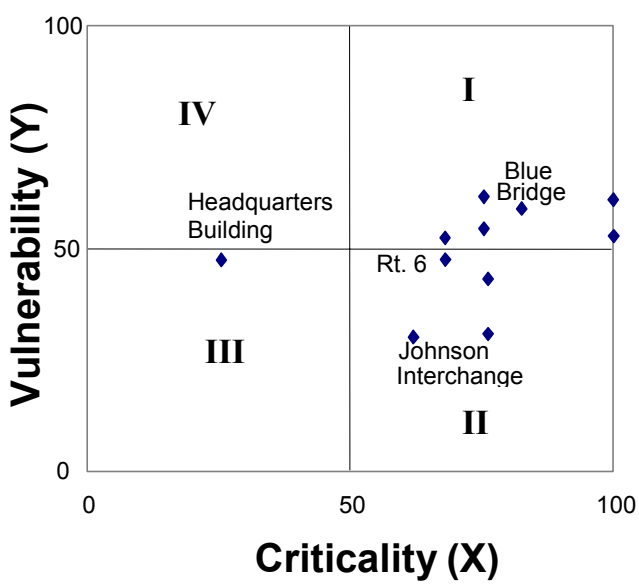


Figure 6 – Illustrative Example of Criticality/Vulnerability Matrix

☑ 3b - Consider consequences for Quadrant I critical assets

Assets that fall into Quadrant I are both critical to the state or region and judged to be vulnerable to the identified threats. The specific consequences of attacks on these assets depend on the nature of the attack and the impact of the loss of the asset to the state or region. Consequences can vary from loss of life and property associated with the attack to loss of an important part of the transportation infrastructure needed to support economic activity, military deployment, or the ability to respond effectively to other emergencies (e.g., loss of an important evacuation route).

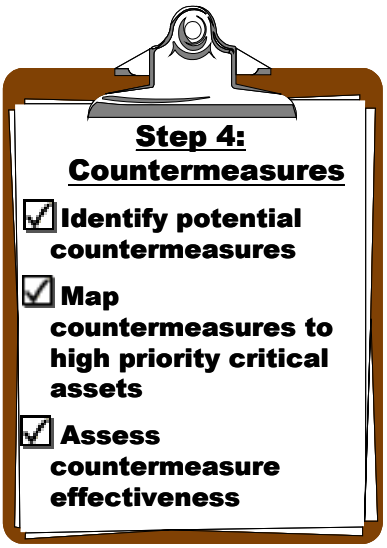
A careful look at the criticality (X) and vulnerability (Y) coordinates of each asset in Quadrant I reveals important information for the consequence assessment of the asset. For example, in the case of Smith Bridge, the asset's X score of 100 is based on the Critical Asset Factors for this bridge, as listed in Table 2, that include high casualty risk, high economic impact, interruption of government continuity and high military importance. The asset's Y score of 57 is arrived based on the Vulnerability Factors and Default Values, as listed in Table 7, that include high level of recognition, open access, no security protection, and high receptor impact. Analyzing these factors provides insights to the consequence assessment for each asset.

In the next step, the vulnerability assessment team should begin with assets in the upper right corner of the matrix and work toward the origin, using their collective experience and judgment to work through the asset list in identifying countermeasures appropriate to the potential consequences.

Step 4 – Countermeasures

Objective

This step identifies typical countermeasures to protect the critical assets from the threats and vulnerabilities assessed previously.



Approach

☑ 4a – Identify potential countermeasures

Developing countermeasures to protect critical assets depends on an effective partnership between engineers and security personnel. Security personnel need to understand the basic approaches the engineers will take in laying out protective systems. Engineers must understand the issues involved with ensuring that anything they design is compatible with security operations and the operations of the asset users. The best way to ensure a viable design is through teamwork.

Countermeasures are developed as a result of the general- and specific-design strategies. They commonly take the form of site-work, building/structure, detection, and procedural elements:

- Site-work elements include the area surrounding a facility or an asset. They can include perimeter barriers, landforms, and standoff distances.
- Building and structure elements are protective measures directly associated with facilities and structures. These elements include walls, doors, windows, and roofs.
- Detection elements detect such things as intruders, weapons, or explosives. They include closed-circuit television, motion detectors, alarms, and weapon and explosive detectors, including chemical and biological weapon detection technologies. These elements can also include the guards used to support this equipment or to perform similar functions.
- Procedural elements are the protective measures required by regulations, policies or plans. These elements provide the foundation for developing the other three elements.

The table below identifies a collection of countermeasures considered applicable to protecting transportation assets, as well as the functionality these countermeasures provide in terms of deterrence, detection, and defense. The terms defined below are

consistent with Army Field Manual 3-19.30 – Physical Security.[5] The implementation of certain countermeasures such as the surveillance systems has to be incorporated into the operation of Intelligent Transportation Systems (ITS) in the DOTs.

- *Deterrence* – A potential aggressor who perceives a risk of being caught may be deterred from attacking an asset. The effectiveness of deterrence varies with the aggressor's sophistication, the asset's attractiveness, and the aggressor's objective.

- *Detection* – Detection senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a response force. A detection system must provide all three of these capabilities to be effective.

- *Defense* – Defensive measures protect an asset from aggression by delaying or preventing an aggressor's movement toward the asset or by shielding the asset from weapons and explosives. Defensive measures: (1) delay aggressors from gaining access by using tools in a forced entry, (2) prevent an aggressor's movement toward an asset, and (3) protect the asset from the effects of tools, weapons, and explosives.

Table 11 - Potential Countermeasures

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.	✓	✓	

[5] "Physical Security" Field Manual, No. 3-19.30, Department of the Army, Washington, DC, 8 January 2001.

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

☑ 4b – Map countermeasures to high-priority critical assets

Using the information from Step 3a, the countermeasures presented in Table 11 are mapped to the high-priority critical assets (i.e., those falling into Quadrant I). The illustrative example in Table 12 provides more information.

Example: Sample State DOT Countermeasures for Bridges

One state DOT identified the following on their list of countermeasures for critical bridges:

- Increased patrol by law enforcement
- Increased patrols by Coast Guard
- Rapid removal of abandoned vehicles
  Barriers around bridge piers
- Construction of barriers around cable anchors (suspension bridges)
- Higher level of identification for personnel working on or around the affected bridge
- Security cameras, monitors and related software to monitor sensitive areas
- Removal of vegetation to provide clear lines of site

☑ 4c – Assess countermeasure effectiveness

The effectiveness of countermeasures is measured subjectively by assessing how well its application reduces either the potential for or consequences of attacks on assets given specific threats and vulnerabilities. In this instance, State DOTs should re-score Steps 1 and 2 to determine whether the proposed countermeasure shifts the consequences (Step 3) into a lower quadrant in Figure 5. If so, Step 5 should be followed to estimate the capital, operating and maintenance costs for the countermeasure as part of a cost-benefit analysis. If the consequences remain the

same, selecting another countermeasure or set of countermeasures should be considered to reduce the threats and vulnerabilities to high-priority critical assets.

Illustrative Example

The following example illustrates the results from Step 4.

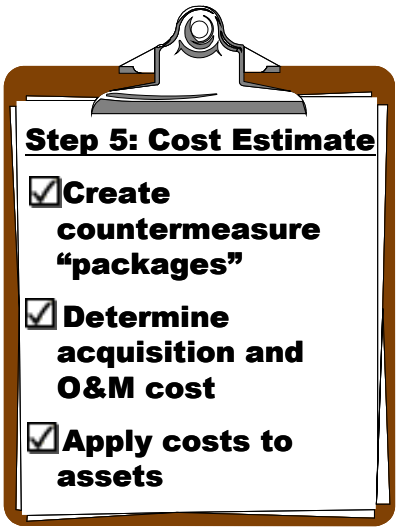
Table 12 – Illustrated Example – Applying Countermeasures to Critical Asset Categories

COUNTERMEASURE	*CRITICAL ASSET CATEGORY*				*COUNTERMEASURE FUNCTION*		
	Infrastructure	Facilities	Equipment	Personnel	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 with 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.	✓	✓			✓	✓	

Step 5 – Cost Estimation

Objective

In this step, general guidelines are provided to calculate the range of costs for implementing the selected countermeasures.



Approach

☑ 5a – Create countermeasure "packages"

The countermeasures identified in Step 4 are intended to deter or detect a potential or real attack or to help defend critical assets in the event an attack is underway. In some cases, the countermeasure will be an action taken to deny access to an asset through physical features or enforcement strategies; in other cases, countermeasures will render the attack harmless or mitigate damages. In many cases, combinations of countermeasures will be needed to achieve the desired vulnerability reduction. This first step in cost estimation is to "package" countermeasures in ways that make sense operationally and from a vulnerability reduction perspective. In some cases, a single measure will apply to multiple assets (e.g., video surveillance may cover multiple transportation assets in high density urban areas); in others, multiple countermeasures will be applied to a single asset (e.g., the vulnerability of a critical bridge or tunnel may be reduced by applying electronic security for intrusion detection as well as physical barriers to deny access to critical structural elements).

This countermeasure "packaging" step will help State DOTs think through procedural, equipment, technological, and structural options for reducing vulnerability. Once viable packages are identified, their unit costs should be determined using standard life cycle costing methods.

☑ 5b – Determine acquisition, operation, and maintenance cost of proposed countermeasures

The capital investment and annual operation and maintenance costs for countermeasures for each highway agency varies widely. It is beyond the scope of this Guide to provide a detailed description of life cycle cost estimation. Nevertheless, Table 13 provides a tool for assigning preliminary costs to each countermeasure listed in this Guide. These costs are described as high (H), medium (M) or low (L). The relative ranges associated with high, medium, and low costs are very subjective and depend on many variables. Sample values are provided in Table 13 as a general guide to categorizing the countermeasure costs. These values are applied to the countermeasures as shown in Table 14.

Table 13 – Countermeasure Relative Cost Range

	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

Table 14 - Estimated Countermeasure Costs

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 any of the most critical type bridges. Elimination of the parking can be accomplished through the use of 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

Example: Arkansas' Countermeasure Cost Estimates
Arkansas provided cost estimates on some specific countermeasures related to fencing, cameras and floodlights.

- 2 TV cameras with floodlights and 200 feet of 10' fence: $23,500
- Fencing off access roads to bridges, installing gates and placing two cameras: $25,000
- 10 cameras with floodlights, gates and 600 feet of fence: $80,000
- 3 cameras with floodlights, gates and 600 feet of fence: $50,000

☑ 5c – Apply costs to assets

This step is the simple application of the unit cost of the countermeasure packages to the critical assets. State DOTs can group assets by asset type (similar to the categories listed in step 1) and extend the unit price for appropriate countermeasures to the number of critical assets in each category. For example, assume a State DOT has identified ten high priority bridges (in terms of their criticality and vulnerability) and the unit cost for the countermeasure package (e.g., intrusion detection, access denial or control, surveillance methods) selected for reducing bridge vulnerability. This unit cost can be applied to the ten critical bridges, recognizing that acquisition, installation, and operation and maintenance may vary from bridge to bridge but the overall cost estimate will provide a reasonable estimate to support investment decisions. A similar process applies to other asset types (e.g., inspection facilities, traffic operations centers) where other countermeasure packages will be applied.

Illustrative Example

Table 15 – Illustrative Example of Countermeasure Costs

CRITICAL ASSET GROUP	*COUNTERMEASURE DESCRIPTION*	*COUNTER-MEASURE FUNCTION*			*ESTIMATED RELATIVE COST (H/M/L*		
		Deter	*Detect*	*Defend*	*Capital*	*Operating*	*Maintenance*
Smith Bridge Blue Bridge	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 any of the most critical type bridges. Elimination of the parking can be accomplished through the use of 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
	Improve lighting	✓	✓		L	L	L

CRITICAL ASSET GROUP	COUNTERMEASURE DESCRIPTION	COUNTER-MEASURE FUNCTION			ESTIMATED RELATIVE COST (H/M/L		
		Deter	Detect	Defend	Capital	Operating	Maintenance
Headquarters Building	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
	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 system.			✓	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	L	L

Step 6 – Security Operational Planning

Objective

This step will improve the security of critical assets by guarding against potential consequences caused by acts of WMD terrorism through security operational planning.

Step 6: Operational Planning

- ☑ **Clarify security planning scope and objectives**
- ☑ **Develop draft operational plan**
- ☑ **Initiate training and exercise activities**

Approach

None of the surveyed State DOTs provided information on security operational planning. The most extensive treatment of this topic comes from the U.S. Department of the Army, which published an updated field manual on physical security.[6] Although much of the information provided here is adapted from that field manual, referencing this manual is encouraged. In addition, the American Public Transportation Association (APTA) has posted on its website a listing of links to transportation related security and preparedness information. This information is available at www.apta.com/info/briefings/brief4_special.pdf.

Physical security is defined as that part of security concerned with physical measures designed to:

- Safeguard personnel,
- Prevent unauthorized access to infrastructure, facilities, equipment, and personnel, and
- Safeguard against espionage, sabotage, damage, and theft.

☑ 6a – Clarify security planning scope and objectives

State DOTs have established emergency plans to prepare for and respond to natural and technological disasters in terms of highway-related services. In most instances, these emergency plans integrate with statewide emergency plans that are consistent with the national disaster framework established in the Federal Response Plan. In the Federal Response Plan, federal assistance to state governments in response to declared emergencies is grouped into twelve functional areas, with a single lead agency responsible for each emergency support function. Many statewide emergency plans also use emergency support functions, assigning the State

Emergency Support Functions

- Transportation
- Communications
- Public Works and Engineering
- Fire Fighting
- Information and Planning
- Mass Care
- Resource Support
- Health and Medical Services
- Urban Search and Rescue
- Hazardous Materials
- Food
- Energy

[6] "Physical Security" Field Manual, No. 3-19.30, Department of the Army, Washington, DC, 8 January 2001.

DOT as the lead agency for transportation. Until recently, the Federal Response Plan (and consequently statewide emergency plans) did not consider acts of WMD terrorism. As such, most State DOTs have not incorporated security operations for WMD terrorism into their established emergency plans.

State DOTs must first define the scope and objectives for security operational planning in light of establishing emergency plans. In general, this activity will confirm the baseline of established emergency plans and will assess any shortfalls or gaps against the criticalities, vulnerabilities and consequences identified in Steps 1-3. As described in Step 6b, State DOTs need to develop a security operational plan to address the shortfalls and gaps identified against their baseline plans.

As noted in Step 2a, the terrorist threat is both dynamic and uncertain. Consequently, the security operational plan must reflect an understanding of how security measures change in anticipation of or in response to specific activities (e.g., special events that may increase the attractiveness of a critical asset as a terrorist target) or reliable information about terrorist activities, either in general or with respect to specific assets and terrorist groups.

☑ 6b– Develop a security operational plan

In order to carry out State DOT roles and responsibilities and maximize U.S. DOT assistance in emergency response situations, substantial transportation resources and plans/procedures must be in place. The overlay of terrorism and WMD on the existing emergency management context introduces a number of new considerations as set forth above. The existing transportation strategies embodied in existing plans may need to be adjusted for characteristics such as scale, lack of lead time, crime scene management, etc. The need for special transportation responses (e.g., quarantining) may be introduced. A set of new hazards for first responders must be a consideration. These and other issues suggest the need to consider appropriate modifications and/or improvements that may be appropriate to the WMD context.

In the illustration below, modeled after the U.S. Army Physical Security Field Manual referenced previously, are several elements that should be included in a security operational plan to protect the critical assets from acts of WMD terrorism. The State DOTs should prepare a security operational plan based on the elements identified below. Note that while the security operational plan outlined below was written with physical facilities in mind (e.g., buildings, military installations), many transportation assets are, in fact “point targets” similar to buildings. State DOTs may determine that, under certain threat conditions, they need to impose access controls and other security measures to protect critical bridges, tunnels, operations centers, and even major interchanges because of their importance or because of their proximity to other critical assets. For example, in the aftermath of September 11th, major arterials in the vicinity of the Pentagon were restricted to passenger vehicles only and both military and law enforcement resources are used to enforce these security measures.

The State DOTs should take the necessary precautions to safeguard their security operation plans and control the distribution and availability of the plan.

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
   - 4.5. Protective lighting system
     - 4.5.1. Use and control
     - 4.5.2. Inspection
     - 4.5.3. Action taken in case of commercial power failure
     - 4.5.4. Action taken in case of failure of alternate power source

4.6. Emergency lighting system
  4.6.1. Stationary
  4.6.2. Portable
4.7. Intrusion Detection System
  4.7.1. Security classification
  4.7.2. Inspection
  4.7.3. Use and monitoring
  4.7.4. Action taken in case of alarm conditions
  4.7.5. Maintenance
  4.7.6. Alarm logs or registers
  4.7.7. Tamper-proof provisions
  4.7.8. Monitor-panel locations
4.8. Communications
  4.8.1. Locations
  4.8.2. Use
  4.8.3. Tests
  4.8.4. Authentication
4.9. Security personnel. General instructions that would apply to all security personnel
  4.9.1. Detailed instructions such as special orders and procedural information should be attached as annexes
  4.9.2. Security personnel include
    4.9.2.1. Composition and organization
    4.9.2.2. Length of assignment
    4.9.2.3. Essential posts and routes
    4.9.2.4. Weapons and equipment
    4.9.2.5. Training
    4.9.2.6. Method of challenging with signs and countersigns
    4.9.2.7. 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

6c – Initiate training and exercise activities.

Good policies, plans, and program development are the beginnings of preparedness. Implementing awareness, training and qualification programs as part of security operational planning helps to determine organizational effectiveness in dealing with a crisis. Experience and data show that training and exercise activities are a practical and efficient way to prepare for crises. They test critical resistance, identify procedural difficulties, and provide a plan for corrective actions to improve crisis and consequence management response capabilities without the penalties that might be incurred in a real crisis. Training and exercise activities also provide a unique learning opportunity to synchronize and integrate cross-functional and intergovernmental emergency response.

Without a common level of awareness, training, or standards, State DOTs and all other responders from the many different organizations and jurisdictions will have difficulty functioning together coherently when confronted by a serious natural, technological, or terrorist incident.

Some elements of a training and exercise program for WMD terrorism include:

- **Awareness –** Understanding the functions of security operational planning in terms of the full range of threats and vulnerabilities faced by an organization.
- **Training –** Implementing and adjusting the security operational plan and developing skills critical to WMD preparedness and response; rehearsing State DOT personnel in their assigned roles and testing whether their response expectations are appropriate. Training can also identify lessons learned, improved standards for performance, and additional resources.
- **Standards –** Identifying which members of an organization have met the required or desired level of training.

Appendix

A. Background

B. Copies of worksheets for all steps

C. Acronym List

D. Bibliography

E. List of individuals contacted

F. Illustrative practices

Vulnerability Assessment Guide Comments

Please provide the following information along with comments:

Last Name *First Name* *Position/Title*

Company/Organization Address

City *State* *ZIP+4*

( ) ( )

Email Address *Business Phone* *Fax Number*

Comments (use additional sheets as necessary):

Please indicate the section(s) of the Guide that your comments address (check all that apply): ❑Introduction, ❑Overview, ❑Critical Assets Identification, ❑Vulnerabilities Assessment, ❑Consequence Assessment, ❑Countermeasures, ❑Cost Estimation, ❑Security Operational Planning, ❑Appendix, or ❑Other

THANK YOU!

PLEASE FAX TO (703) 676-0884,

Attn: Shahed Rowshan

If You Have Any Questions, Please Call (703) 676-0848