

NCHRP PROJECT 20-59(28)

SECURITY 101: A PHYSICAL SECURITY PRIMER FOR TRANSPORTATION AGENCIES

Presentation to

*Transportation Hazards & Security
Summit and Workshop 2010*

Wednesday, August 25, 2010

Beckman Center of the National Academy
of Sciences and Engineering Irvine,
California



*Countermeasures Assessment &
Security Experts, LLC*

110 Quigley Boulevard

Airport Park

New Castle, DE 19720

302-322-9600

20-59(28) IS AN INTRODUCTORY REFERENCE DOCUMENT

The objective of this project is to provide transportation managers and employees with an introductory-level reference document to enhance their working knowledge of security concepts, guidelines, definitions, and standards.

It is anticipated that the primary user group for this report is transportation personnel without a security background whose work requires them to address, perform, or supervise security activities as part of their overall job responsibilities.

However, although designed for those with minimal or no formal security training, the report is also a handy reference guide sufficiently detailed to be of use to security professionals as well.

20-59(28)

TABLE OF CONTENTS

- Chapter 1 – Risk Management and Risk Assessment
- Chapter 2 – Plans and Strategies
- Chapter 3 – Physical Security Countermeasures
- Chapter 4 – Security Personnel and Training
- Chapter 5 – Infrastructure Protection
- Chapter 6 – Homeland Security
- Appendix A – Annotated Bibliography
- Appendix B – Additional Sources of Information
- Appendix C – List of Acronyms and Abbreviations
- Appendix D – Glossary of Terms and Definitions

RISK MANAGEMENT

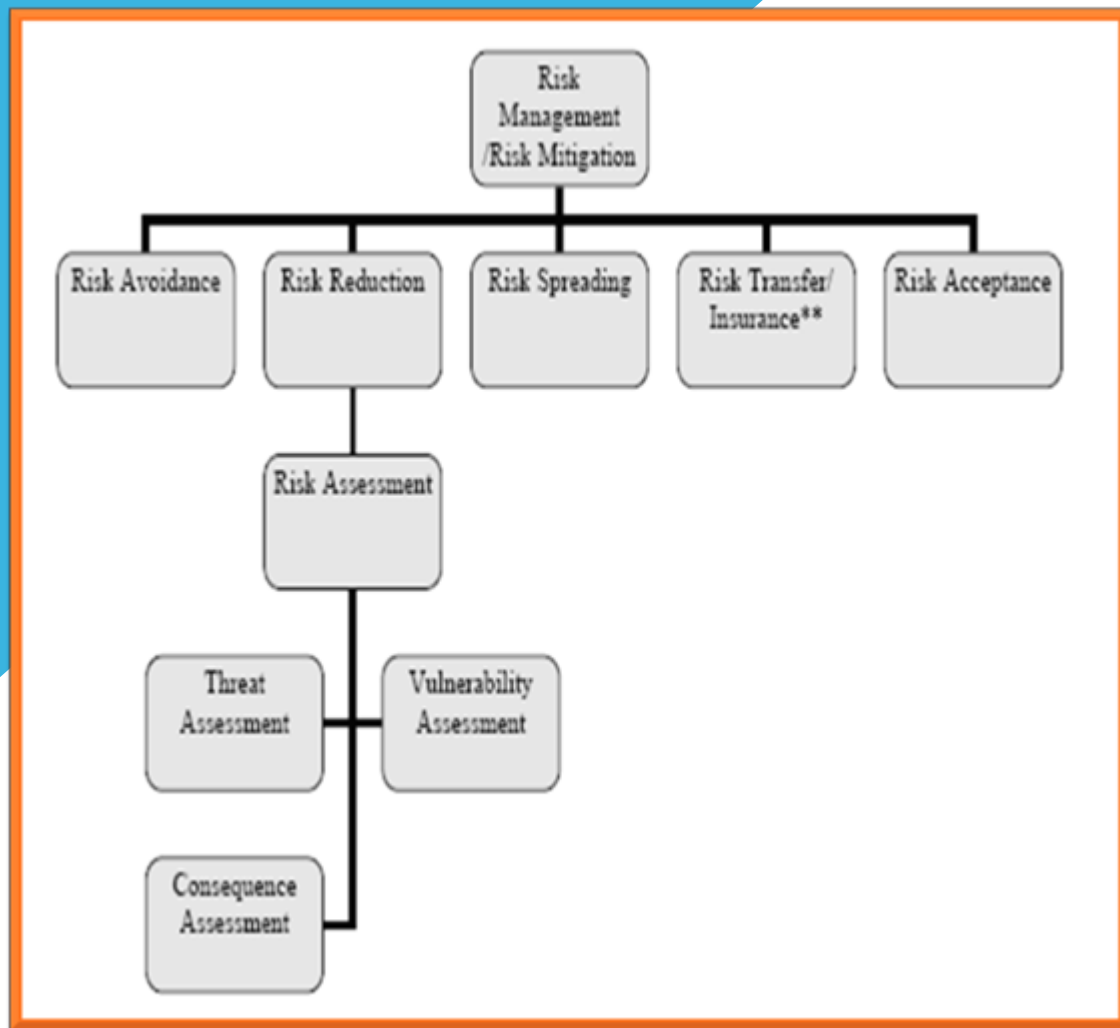
Risk Avoidance

Risk Reduction

Risk Spreading

Risk Transfer

Risk Acceptance



CHAPTER 1: FIGURE 1: Risk Management Spectrum

Adapted from *Vulnerability Assessment of Physical Protection Systems* –
Mary Lynn Garcia Sandia National Laboratories

Risk Assessment

- Threat Assessment
- Vulnerability Assessment
- Consequence Assessment

RISK REDUCTION

RISK IS A FUNCTION OF VULNERABILITY AND CONSEQUENCE

$$\text{Risk} = [\text{Threat} \times \text{Vulnerability}] \times \text{Consequence}$$

Threat is a measure of the likelihood that a specific type of attack will be initiated against a specific target

Vulnerability is a measure of the likelihood that various types of safeguards against threat scenarios will fail

Consequence is the magnitude of the negative effects if the attack is successful

CHAPTER 1: FIGURE 2: Risk Equation

Source: *Volpe Risk Assessment and Prioritization*, Volpe Journal 2003

THREAT ASSESSMENT

Threat Description	
	Pipe Bomb
	Suicide Belt
	Suicide Vest
	Briefcase/Suitcase Bomb
	Compact Sedan
	Sedan
	Passenger/Cargo Van

Explosives

- There are two methods of delivery of CE's or IED's that deserve particular attention – Vehicle Borne Improvised Explosives Devices (VBIED's) and Suicide Bombings.
- According to the State Department's Bureau of Diplomatic Security VBIED's are "far and away the weapon of choice for terrorist attacks."

CHAPTER 1: TABLE 1: Evacuation Distance Threat & Explosive Mass

Cropped and Adapted from *Improvised Explosive Device Safe Standoff Distance Cheat Sheet*, NGIC, US Army (Unclassified)

CATEGORY A and CATEGORY B - BIOLOGICAL THREAT AGENTS

Table 2. Onset, Health Impacts, and Treatments for Some Agents of Concern

Disease (agent)	Incubation period*	Symptoms
HIGH THREAT AGENTS (CATEGORY A)		
Anthrax (<i>Bacillus anthracis</i>) (inhalational)	typically 1–6 days, but up to 42	Fever, cough, profound sweats malaise, fatigue, myalgias
Plague (<i>Yersinia pestis</i>)	1–7 days (usually 2–3 days)	Fever, cough, shortness of breath, sore lymph nodes
Tularemia (<i>Francisella tularensis</i>)	1–21 days (avg 3–6)	Fever, cough, ...
Marburg (Viral hemorrhagic fever)	4–21 days	... diarrhea, ... bleeding in severe cases
Ebola (Viral hemorrhagic fever)	4–16 days	... onset, fever, headache, ... followed by vomiting and diarrhea, rash, generalized bleeding in severe cases
Smallpox (Variola)	... (avg 12)	Fever, aches, after 2–4 days rash appears
Botulism (Botulinum toxin)	12 hours–5 days	Muscle paralyzing illness
LOWER THREAT AGENTS (SELECTED CATEGORY B AGENTS)		
Cholera (<i>Vibrio cholerae</i>)	4 hours–5 days (usually 2–3 days)	Sudden onset of voluminous watery diarrhea, vomiting, cramps, dehydration
Glanders (<i>Burkholderia mallei</i>)	1–14 days via aerosol	Pneumonia with or without blood poisoning, ulcers in nose, mouth, throat and lungs
Q fever (<i>Coxiella burnetii</i>)	7–41 days	Flu-like illness that can lead to pneumonia and hepatitis
Encephalitis (Alphaviruses)	2–6 days	Fever, aches, pain behind the eye, nausea, vomiting
Ricin (<i>Ricinus communis</i>)	18–24 hours	Can shut down organ function

Weapons of Mass Destruction

CHAPTER 1: TABLE 4: Onset, Health Impacts, and Treatments

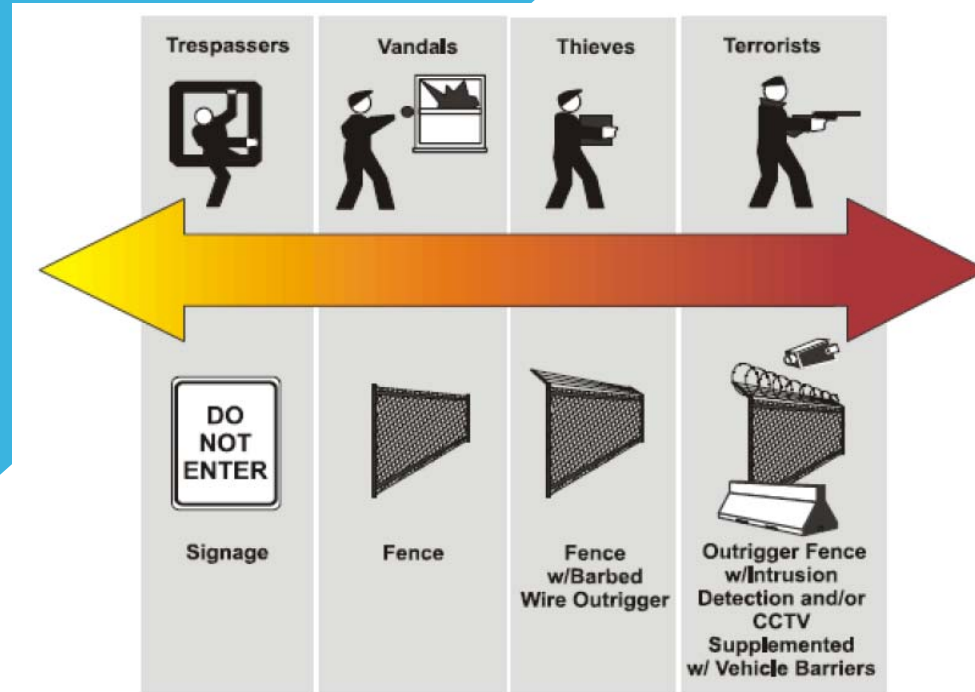
Source: *Biological Attack Human Pathogens, Biotoxins, and Agricultural Threats*, National Academy of Sciences 2005

As a part of the Department of Defense Unified Facilities Criteria (UFC), DOD published *Security Engineering Facilities Planning Manual Draft UFC 4-020-01* in March 2006. The UFC presents four major aggressor objectives that describe aggressor behavior.

- Inflicting injury or death on people
- Destroying or damaging facilities, property, equipment, or resources
- Stealing equipment, material, or information
- Creating adverse publicity

The three broad categories of aggressors are criminals, protesters and terrorists.

ADVERSARY TYPES (AGGRESSOR)



CHAPTER 1: FIGURE 4: Security Countermeasures by Type of Adversary

Source: *Security Design Considerations*, Federal Transit Administration 2004

SECURITY SURVEYS



- ✓ “The survey is a fact gathering question based process that uses various data collection tools to obtain necessary information about the characteristics of the organization, its systems and operations, and the consequences to the organization that would result from a successful attack against identified threat targets.”
- ✓ “The efficacy of this report will be determined primarily by the comprehensiveness and derivation of facts and opinions produced by the conduct of interviews, examinations, observations, analysis and investigations.”

OBJECTIVES AND BENEFITS OF A SECURITY PLAN

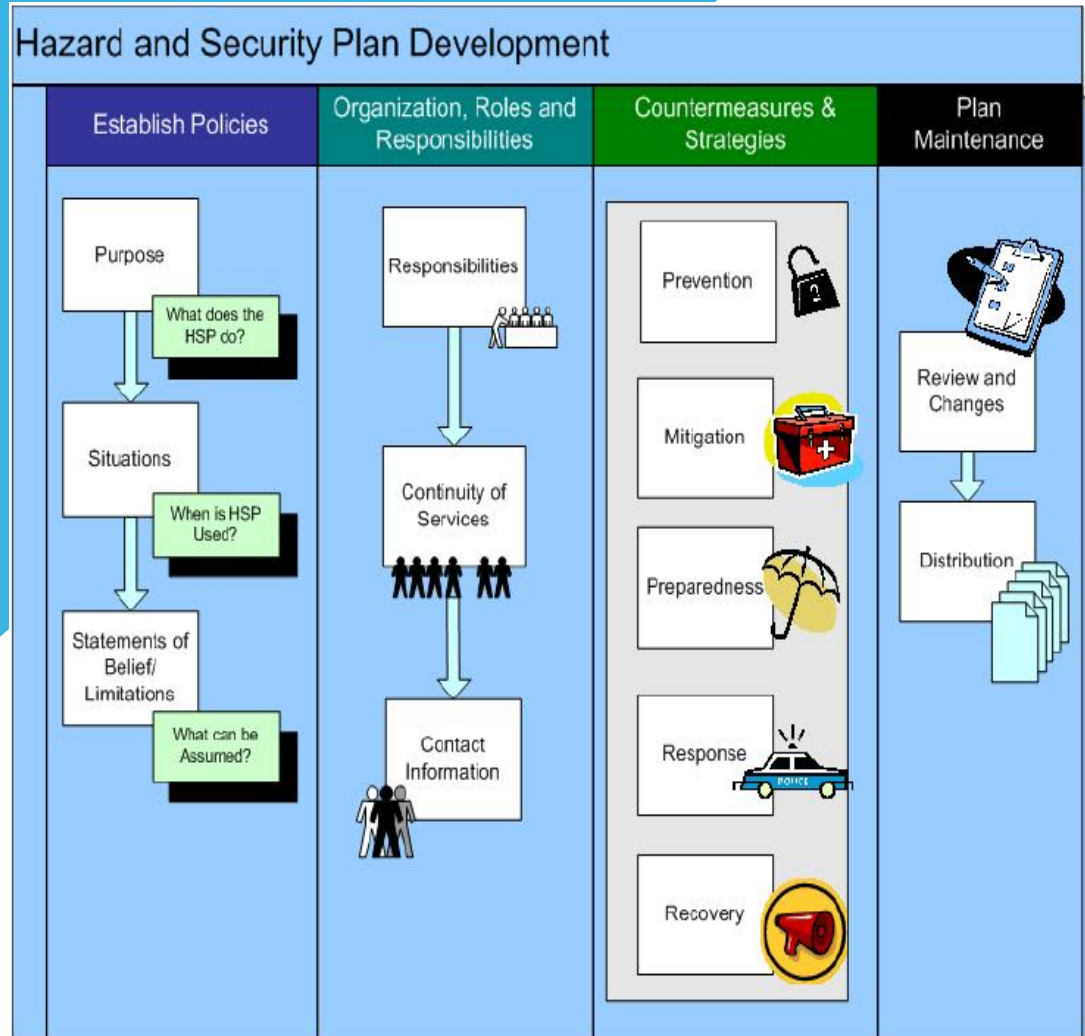
“The security plan directs personnel towards prevention and mitigation of the effects of security incidents by integrating those approaches that have proven to be effective into the operating environment.”



CHAPTER 2: FIGURE 7:
Security Plan Benefits

ELEMENTS OF A SECURITY PLAN

“TCRP Report 86 Volume 10, Hazard and Security Plan Workshop provides an excellent overview of the transportation security planning process. The document also presents a template for Hazard and Security Plan (HSP) development. The template describes the four core planning development functions: (1) establish priorities (2) organization roles and responsibilities (3) countermeasures and strategies, and (4) plan maintenance.”

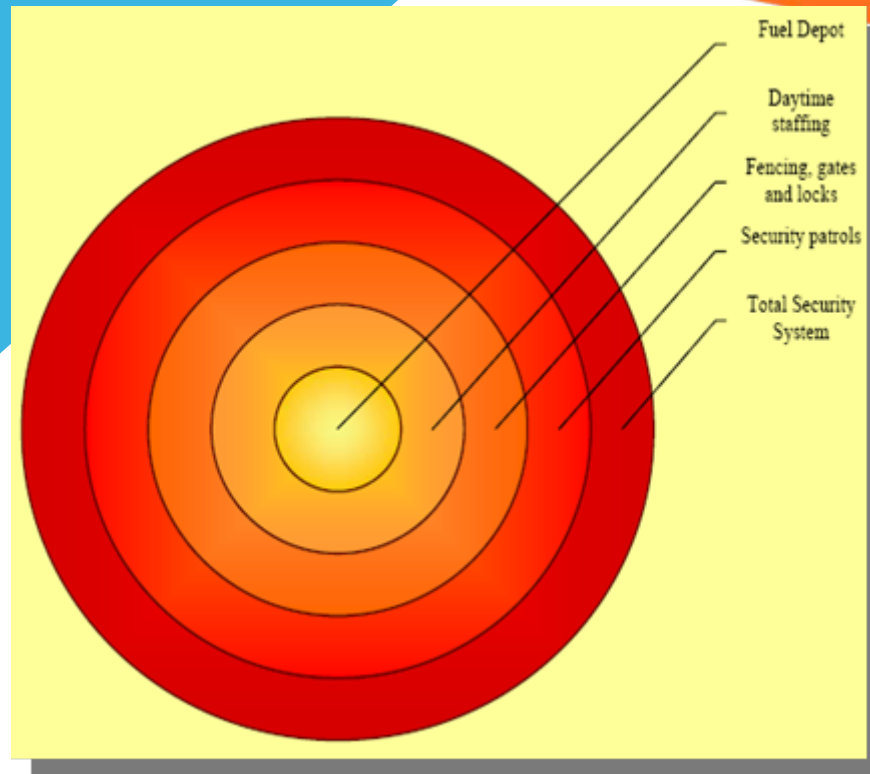


CHAPTER 2: FIGURE 8: Hazard and Security Plan Development

Source: TCRP Report 86 Volume 10, *Public Transportation Security Hazard and Security Plan Workshop* 2006

LAYERED SECURITY

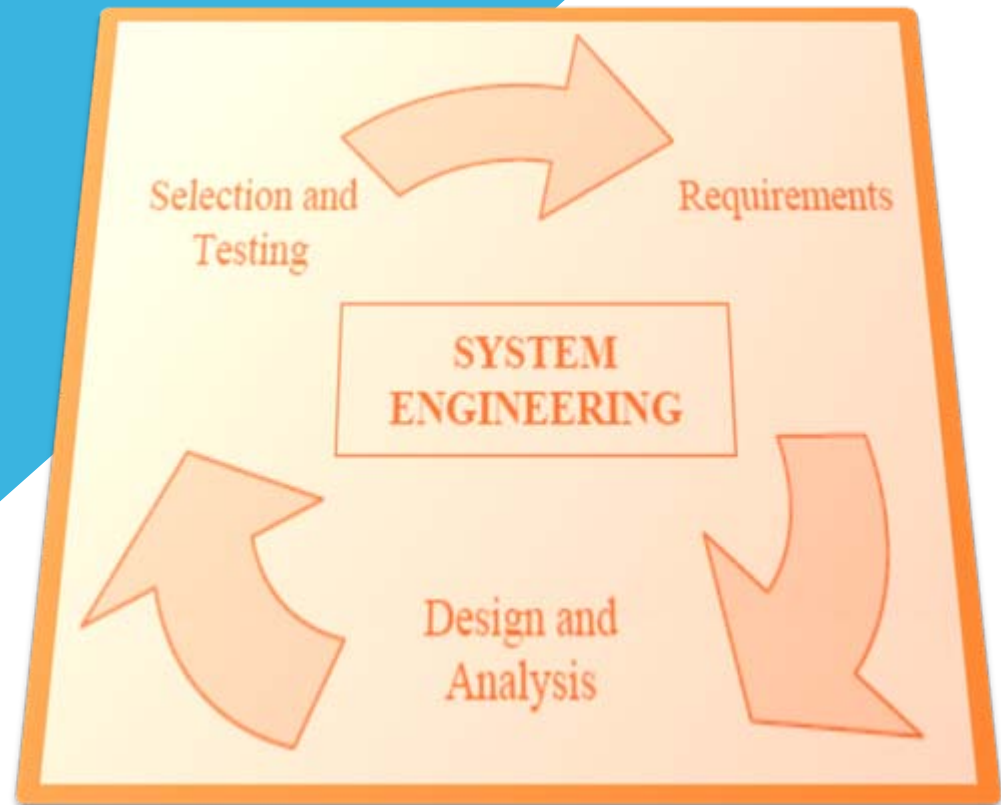
Changing characteristics, conditions and events require the synthesis of available resources as a means to compensate for the weaknesses or loss of capabilities of one security countermeasure for the other. This concept of “layered security” that can also be referred to as overlapping security provides security design strategists with the means to overcome uncertainty in security resource allocation and decision-making.



**CHAPTER 2: FIGURE 12:
Fuel Depot Layered Security**

INTEGRATED SYSTEM SECURITY

“Security related system engineering is defined as the protection of physical infrastructure components and logical structures and processes from threats and vulnerabilities. (Garcia 2001) The process begins with problem definition, continues through to consideration of multiple potential solutions and ends with analysis and selection of the best design to meet requirements and goals.”



Chapter 2: FIGURE 13:
System Engineering

SECURITY COUNTERMEASURES

SIGNS



U.S. Army Corps of Engineers Sign
Standards Manual EP 310-1-6a and
EP 310-1-6b

"The manual provides a Checklist of Sign Plan Elements that depicts the steps necessary to implement an effective sign plan. The checklist includes: (1) an inventory of existing signs and their condition, (2) collection or development of up to date pictorials, maps (optimally supported by GIS), diagrams, blueprints, or other representation of the area in need of protecting, (3) preparation of the site plan and sign layout materials, and (4) implementation of the plan in conformance with the guidelines established."

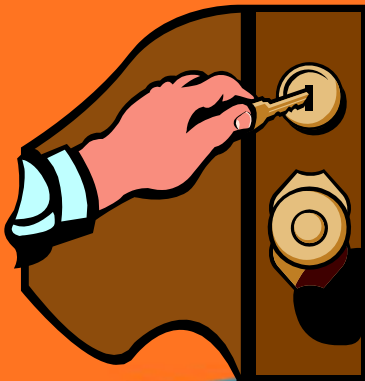
CHAPTER 3: FIGURE 16: Security Signs

Source <http://www.safetysign.com>

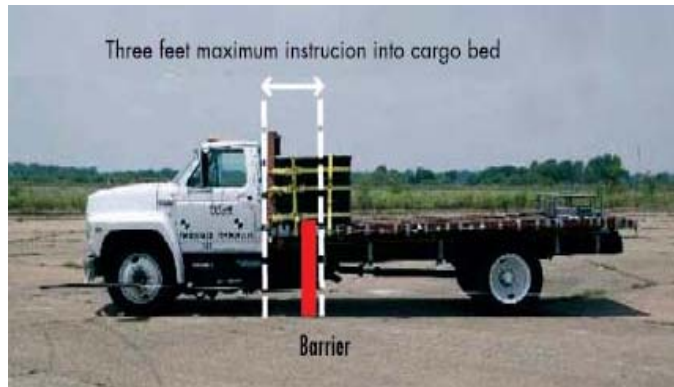
SECURITY COUNTERMEASURES

KEY CONTROL AND LOCKS

According to the *US Army Field Manual 19-30, Chapter 8* most key locks and conventional combination locks can be picked by an expert in a matter of minutes. More sophisticated manipulation resistant locks, locks with four or more tumblers, some interchangeable core systems, or relocking devices on safes or doors can provide an “appreciable increase” in difficulty but are still subject to compromise.



Performance standards for locks based on these capabilities exist through ANSI/BHMAA Series 156 and United Laboratories (UL) 1034, 437, 768, 294, 2058 and 305. It is recommended that the agency consult with a professional locksmith for mechanical locks or security professional for electromechanical or electromagnetic locks before spending security dollars on new hardware or upgrades.



SECURITY COUNTERMEASURES FENCING

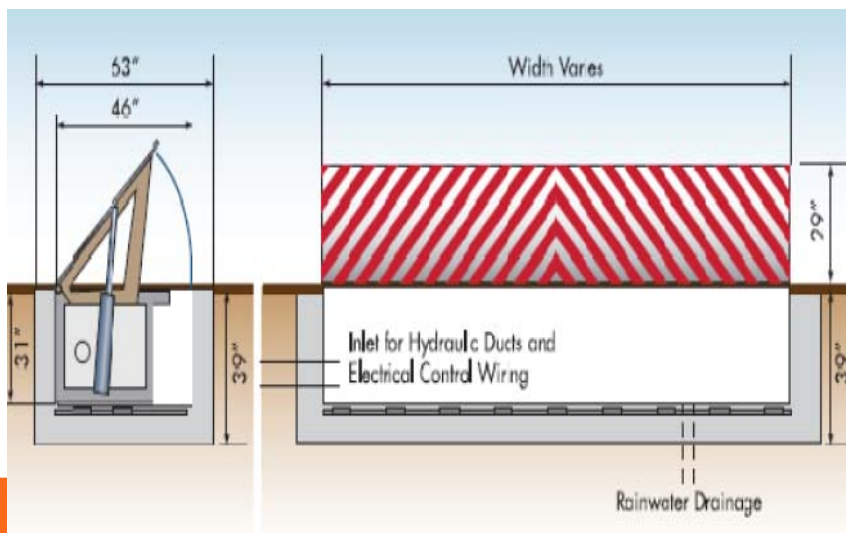
“K Certification anti-ram standards originated at the Department of State. The rating is determined from perpendicular barrier impact results of a truck weighing 15,000lb (6810kg) striking the barrier straight on. To meet the standard the truck’s cargo bed cannot penetrate the barrier by more than 1 meter. Table 8 and Figure 18 depict the vehicle and crash ratings associated with the truck striking the barriers at speeds of 30mph, 40mph and 50mph.”

CHAPTER 3: Figure 18: Truck Striking Barrier

Source FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

SECURITY COUNTERMEASURES

PROTECTIVE BARRIERS



CHAPTER 3: FIGURE 23 AND 24: Mobile Wedge Barrier

Source FEMA 430, *Building, Site and Layout Design Guidance to Mitigate Potential Terrorist Attacks*, 2007

SECURITY COUNTERMEASURES

PROTECTIVE LIGHTING



“Protective lighting security planning requires thoughtful and careful study to ensure that the benefits of the program are maximized. In particular ... dual use aspects of lighting should be examined for potential integration into mainstream transportation operations. And vice versa the security applicability of agency lighting configurations should be factored into operational planning and decision making.”

CHAPTER 3: TABLE 9: Lamp Type, Life and Efficiency

Source Adapted from NFPA 730 Guide for Premises Security, 2006

Type of Lamp	Lamp Life	Lamp Efficiency
Incandescent	500 – 4000 hours	17 – 22 Lumens Per Watt
Fluorescent	9,000 – 17,000 hours	67 – 100 Lumens Per Watt
[HID]		
Mercury Vapor	24,000+ hours	31 – 63 Lumens Per Watt
Metal Halide	6,000 hours	80 – 115 Lumens Per Watt
High Pressure Sodium	24,000 hours	80 – 140 Lumens Per Watt

Security Countermeasures

ALARM SYSTEMS



The main elements of an intrusion detection alarm system include:

- Sensors
- Alarm processor
- Monitoring system
- Communications architecture

The components of an alarm system include:

- Main Control Unit
- Keypad
- Input Devices (Sensors)
- Transformer
- Power Supply
- Telecommunications

SECURITY COUNTERMEASURES

ACCESS CONTROL SYSTEMS



CHAPTER 3: FIGURE 28:
Cipher Access Control Barrier

Source SAVER Summary, Handbook of Access Control Technologies,
2005



CHAPTER 3: FIGURE 29:
**Token-based Drop Arm Barrier
System**

Source SAVER Summary, Handbook of Access Control
Technologies, 2005

Security Countermeasures

ACCESS CONTROL SYSTEMS

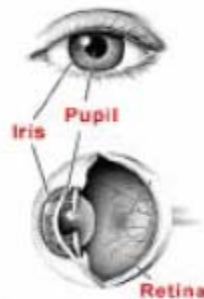


Figure 1: Iris Diagram²



Figure 2: Iris Structure.³



Figure 1: Minutiae⁵



Figure 2: Other Fingerprint Characteristics⁴

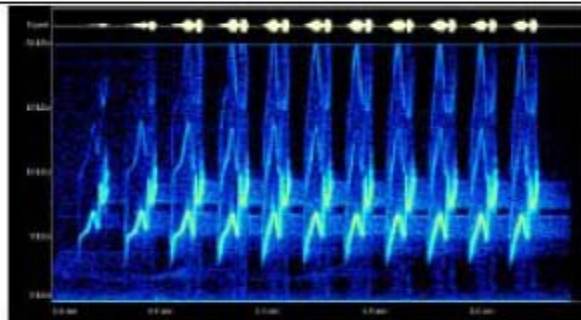
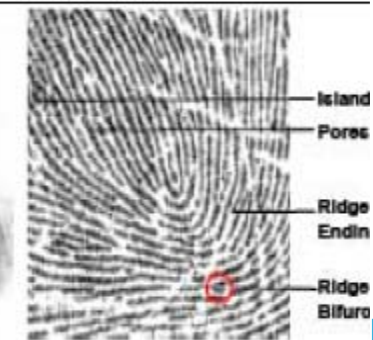
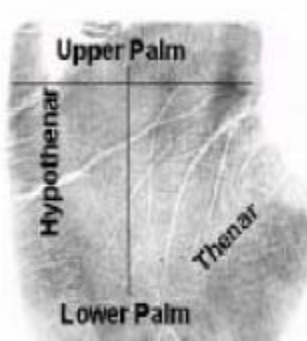


Figure 1: Voice Sample: The voice input signal (top of image) shows the loudness with respect to the time domain. The lower image (blue) depicts spectral information of the voice signal. This information is plotted by displaying the time versus the frequency variations.¹⁰



CHAPTER 3: FIGURE 30:

Biometric Technologies Including Iris Recognition, Fingerprint Identification, Voice Recognition and Palm Print Identification

Source: Adapted from National Science and Technology Council (NSTC) Subcommittee on Biometrics
<http://www.biometricscatalog.org/NSTCSubcommittee>

“In 2007 the American Public Transportation Association (APTA) published The Selection of Cameras, Digital Recording Systems, Digital High Speed Train-lines and Networks for Use in Transit Related CCTV Systems, as a part of its IT Standards Program Recommended Practice (RP) Series. APTA IT-RP-001-07 V1.2 is a valuable technical resource for transportation agencies considering implementation or upgrading of CCTV systems. The document covers the selection and use of cameras for CCTV at stations as well as on moving transportation conveyances such as buses or train cars. Recording devices and backbone architecture for support of CCTV are discussed in detail.”

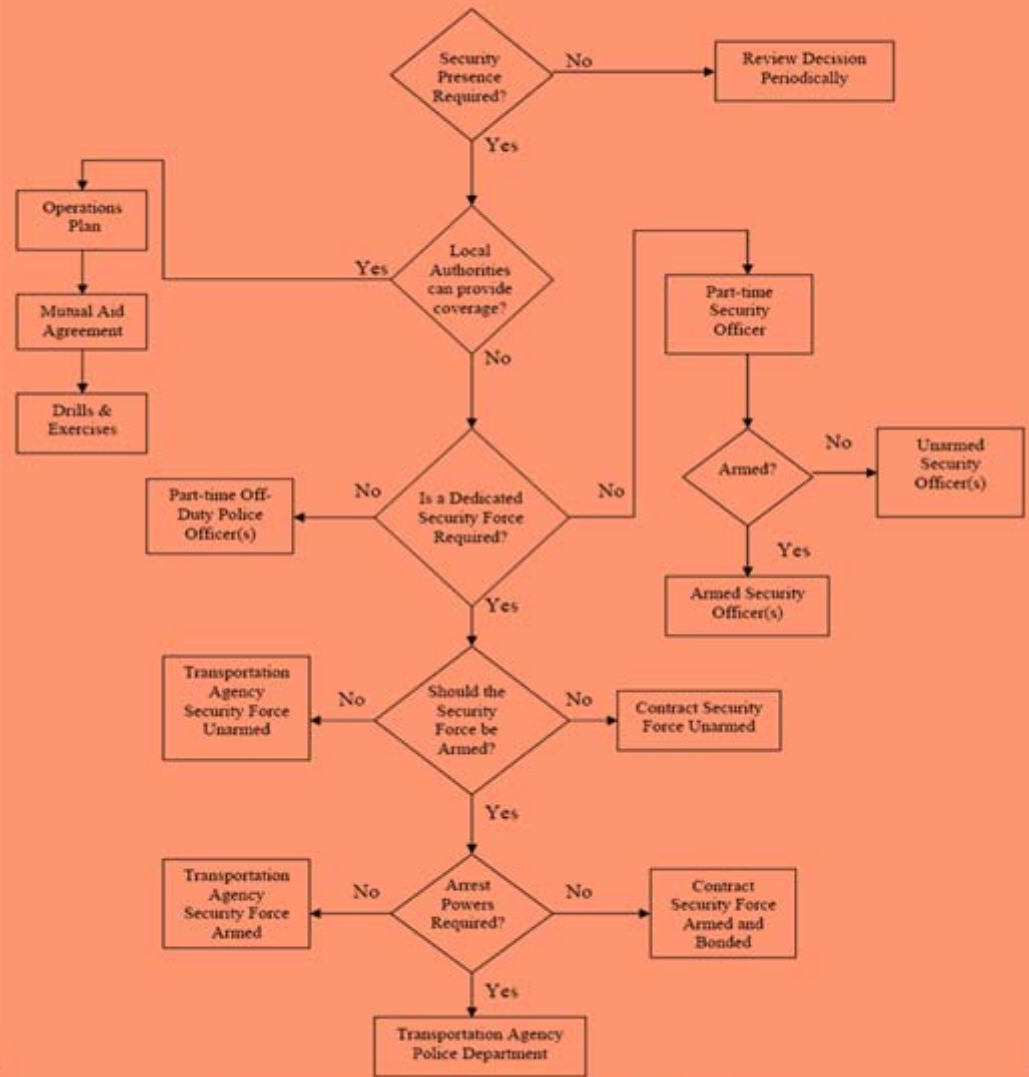
SECURITY COUNTERMEASURES SURVEILLANCE SYSTEMS AND MONITORING



“Security personnel bring the capacity to perceive the true nature of a threat and to recognize on-going aggressor tactics. When adequately armed or reinforced they can repel or overcome the use of deadly force by responding with equal or greater force to neutralize the threat or activity. This factor alone is predominating in both the homeland security and public safety context. Absent a response force aggressors or criminals would quickly disregard other security countermeasures as irrelevant.”



TRANSPORTATION SECURITY FORCE PLANNING FLOW CHART



Copyright © 2008 Countermeasures Assessment & Security Experts, LLC - All Rights Reserved

SECURITY COUNTERMEASURES SECURITY FORCES

“Irrespective of what underlying qualitative factors drive the decision about fielding security personnel, the best way to accurately make staffing level determinations is through the use of quantitative analysis. There are two different sets of quantifying data that are available, (1) security breach or crime incident based information including both calls for service and self-initiated incident responses, and (2) policy and procedure supported staffing deployment that is activity and scenario driven.”



IN THOSE AGENCIES WITHOUT A DEDICATED SECURITY FORCE A COMMITTEE OF DEPARTMENT SECURITY COORDINATORS SHOULD BE EMPOWERED WITH THE AUTHORITY TO MANAGE SECURITY ACTIVITIES SYSTEM WIDE. THERE ARE THREE KEY AREAS OF PROGRAM COORDINATION:

SECURITY COMMITTEES

- To deploy a broad based system wide security management process that identifies, tracks and responds to all security threats, vulnerabilities and occurrences.
- To maintain a workplace where security incidents are routinely reported and contributions to improve security are received from every staff and operating department.
- To ensure that front line and mid-management employees promote security awareness and communications throughout the organization.

“Employees ... are often the first to observe that something is wrong. But transportation agencies cannot assume that employees will focus upon security issues without training. There is a need for employees to receive security awareness orientation to prepare them for their security roles.”

SECURITY AWARENESS

CHAPTER 4: FIGURE 39: FBI Advisory

Source: Federal Bureau of Investigation

FBI Advisory

If you receive a suspicious letter or package
What should you do?



- 1 Handle with care**
Don't shake or bump
- 2 Isolate and look for indicators**
- 3 Don't Open, Smell or Taste**
- 4 Treat it as Suspect!**
Call 911

If parcel is open and/or a threat is identified...

For a Bomb	For Radiological	For Biological or Chemical
Evacuate immediately Call 911 (Police) Contact local FBI	Limit Exposure - Don't Handle Distance (Evacuate area) Shield yourself from object Call 911 (Police) Contact local FBI	Isolate - Don't Handle Call 911 (Police) Wash your hands with soap and warm water Contact local FBI

 Police Department _____
Fire Department _____
Local FBI Office _____
(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

SECURITY TRAINING



Utility/Purpose	
Discussion-Based Exercises	Familiarize players with current plans, policies, agreements, and procedures; develop new plans, policies, agreements, and procedures
Seminar	Provide overview of new or current plans, resources, strategies, concepts or ideas
Workshop	Achieve specific goal or build product (e.g., exercise objectives, SOPs, policies, plans)
Tabletop Exercise (TTX)	Validate plans and procedures by utilizing a hypothetical scenario to drive participant discussions
Game	Explore decision-making process and examine consequences of those decisions
Operations-Based Exercises	Validate plans, policies, agreements, and procedures; clarify roles and responsibilities; identify resource gaps
Drill	Validate a single operation or function of an agency
Functional Exercise (FE)	Evaluate capabilities, functions, plans, and staffs of Incident Command, Unified Command, intelligence centers, or other multi-agency coordination centers (e.g., EOCs)
Full-Scale Exercise (FSE)	Validate plans, policies, procedures, and cooperative agreements developed in previous exercises through their actual implementation and execution during a simulated scenario; includes actual mobilization of resources, conduct of operations, and integrated elements of functional exercise play (e.g., EOCs, command posts)

CHAPTER 4: FIGURES 41 and 42: Security Exercise Types by Planning/Training Requirements

Source: DHS Homeland Security Exercise and Evaluation Program Guidance Documents (HSEEP Vol# I, II, III, IV, and V)

INFRASTRUCTURE PROTECTION

Factors Can Include:

- casualty impact
- business continuity
- economic impact
- replacement cost
- replacement downtime
- redundancy
- symbolic importance



Once each asset has been delineated the categories of personnel (human), property (physical) or information (cyber) can be used to group the individual elements so that the second “factoring” aspect of the critical infrastructure identification process can be accomplished. Factors can refer to any number of important issue areas so long as they are relevant to the agency performing the analysis.

INFRASTRUCTURE PROTECTION

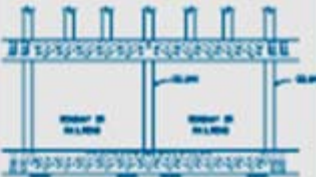
BUILDING SECURITY STANDARDS

1. Vulnerability Assessment of Federal Facilities, DOJ 1995
2. ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, ISC May 2001
3. ISC Security Standards for Leased Space, ISC 2004
4. GSA Lease Security Standards, GSA November 2005
5. Standard Guide for Developing a Cost-Effective Risk Mitigation Plan for New and Existing Constructed Facilities: E 2506 – 06 ASTM Committee on Standards, Copyright © 2006 ASTM International www.astm.org
6. GSA Facilities Standards for the Public Buildings Service General Services Administration March 2005 <http://www.gsa.gov>
7. DoD Minimum Antiterrorism Standards for Buildings (Unified Facilities Criteria UFC 4-010-01) Department of Defense October 2003
www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf
8. DoD Security Engineering Facilities Planning Manual (Draft) UFC 4-020-01 Department of Defense March 2006 www.wbdg.org/ndbm/DesignGuid/pdf/Final%20Draft_UFC_4-020-01.pdf



While the infrastructure of the entire route is an important part of transportation agency security planning, bridges and tunnels by virtue of their engineering, placement or cost often are among the most critical assets of the agency.

BRIDGES AND TUNNELS

Type	Description	Sketch
Immersed Tube Tunnel	- Employed to traverse a water body - Preconstructed sections are placed in a pre-excavated trench and connected - Typical materials include steel and concrete immersed tunnel sections - After placement, tunnel is covered with soil	
Cut-and-Cover Tunnel	- In urban areas - Excavated from the surface, then constructed in place and backfill placed to bury structure - For subway line structures, subway stations, and subsurface highway structures - Typically concrete cast-in-place or precast sections - Steel framing and concrete fill	
Bored or Mined Tunnel	- In urban or remote locations in land, on mountains, or through water bodies - Bored using a variety of techniques - Supported by initial and final support systems - Soft ground or rock tunneling - Structure may have various liner systems, including rock reinforcement, shotcrete, steel ribs and lattice girder, precast concrete segment, cast-in-place concrete, and fabricated steel lining	
Air-Rights Structure Tunnel	- In urban areas - Created when a structure is built over a roadway or trainway using the roadway's or trainway's air rights - The limits that an air-rights structure imposes on the emergency accessibility and function of the roadway or trainway that is located beneath the structure should be assessed	

CHAPTER 5: FIGURE 47:
Transportation Tunnel Types

Source: NCHRP Report 525: Volume 12 – Making Transportation Tunnels Safe and Secure, 2006

INFRASTRUCTURE PROTECTION

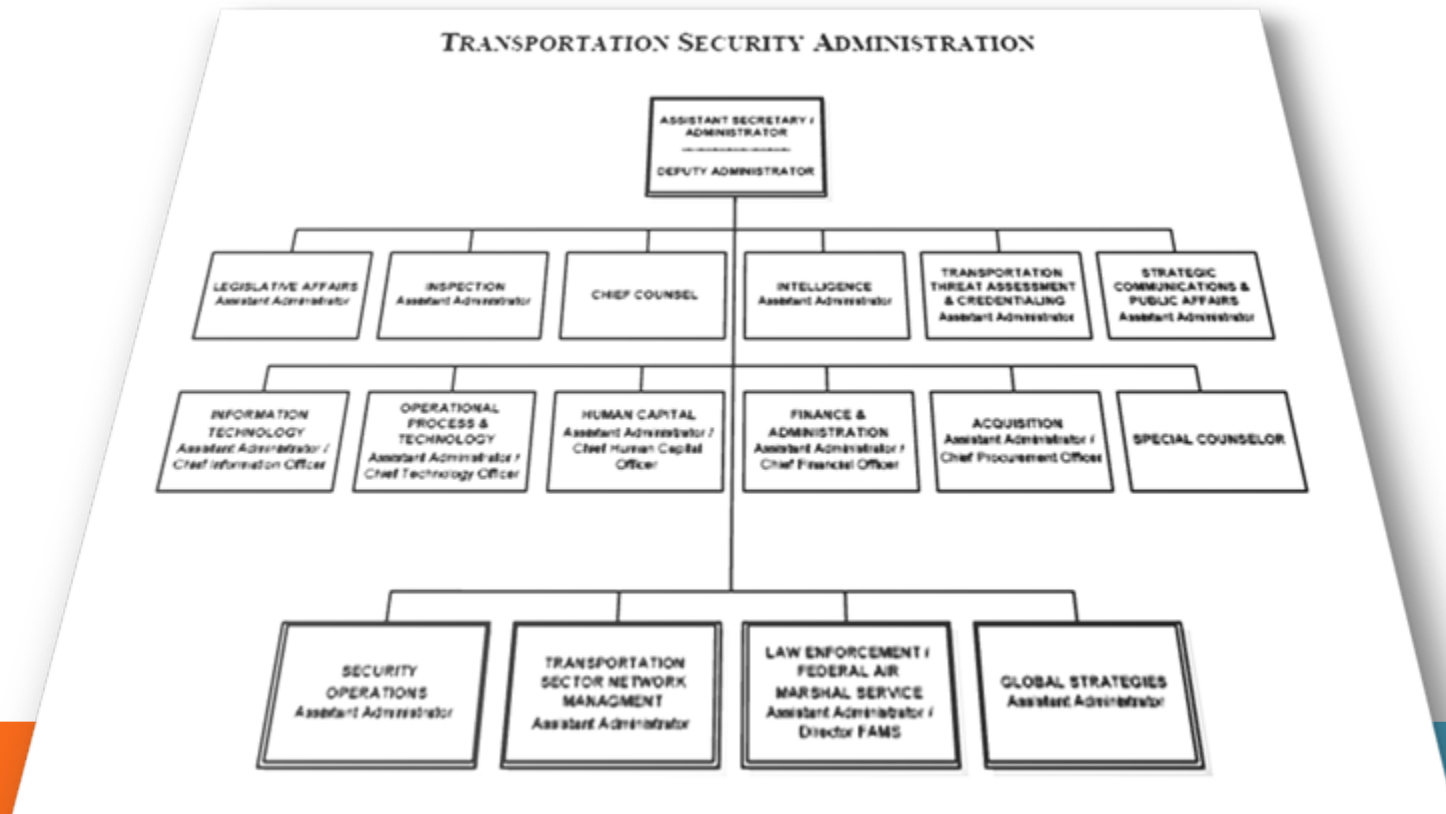
ROLLING STOCK AND VEHICLES

“Transportation vehicle security today comprises two main areas: (1) the safety and protection of vehicles, passengers or occupants; and (2) avoiding the use of the conveyance as a weapon of destruction or mass destruction (WMD).”

“The short-line freight railroad industry is currently engaged in conducting vulnerability assessments and security planning focused towards preventing, eliminating, reducing or mitigating the potential use of the freight rail system as a target for terrorism or criminal attack; or as a delivery system for a weapon of mass destruction. The program is partially funded by DHS grants under the FY08 Freight Railroad Security Grant Program (FRSGP). The planning is intended to address the transportation of Toxic Inhalation Hazards (TIH) within high population density areas.”



HOMELAND SECURITY LAWS AND STATUTES



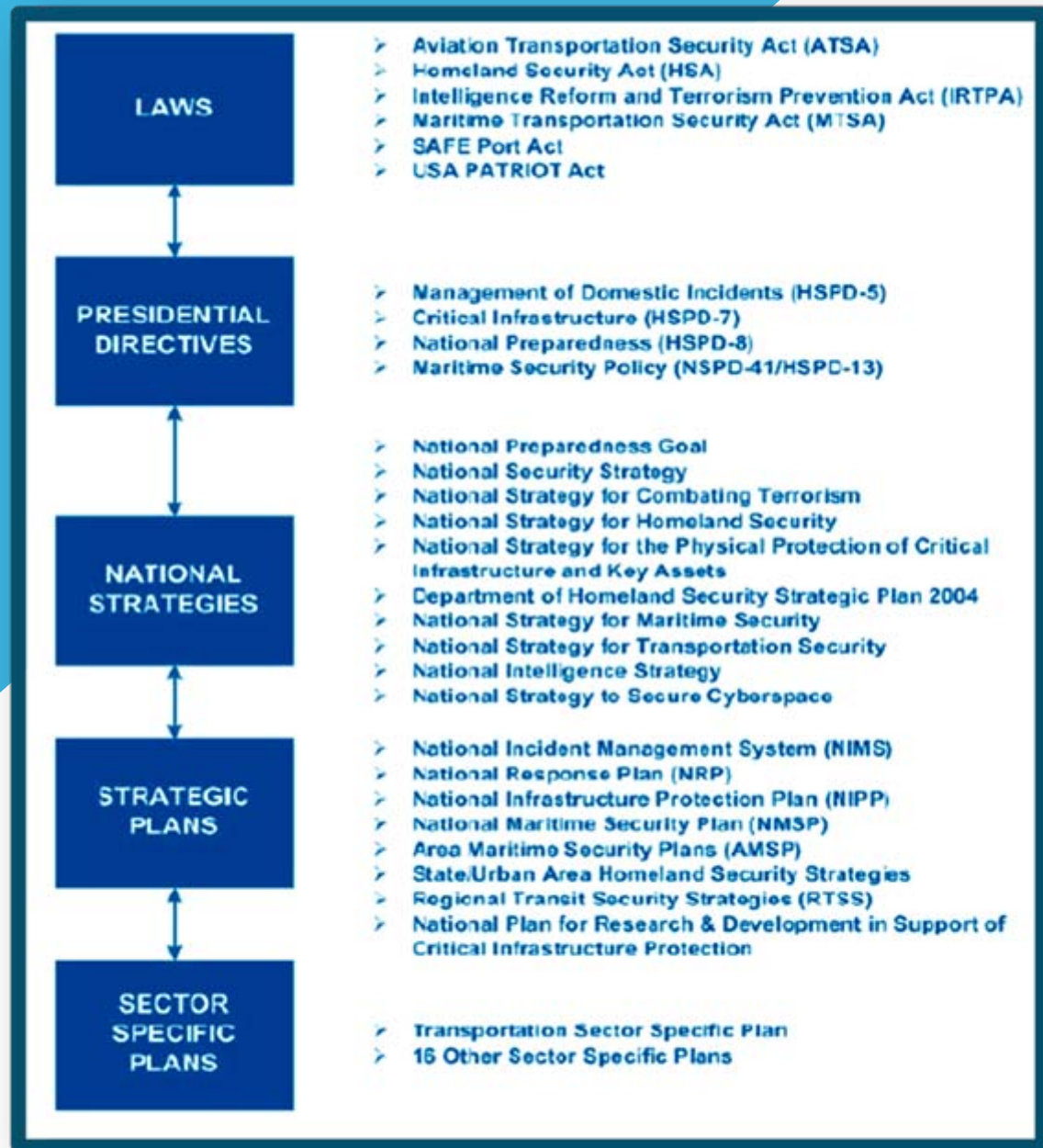
CHAPTER 6: FIGURE 50:
Transportation Security Administration
Organization Chart, March 20, 2008

Source: www.dhs.gov

HOMELAND SECURITY

NATIONAL PREPAREDNESS ARCHITECTURE

Components important to transportation include: (1) National Strategy for Homeland Security; (2) National Strategy for Transportation Security; (3) National Strategy for Maritime Security; (4) National Response Framework; (5) National Incident Management System; (6) National Infrastructure Protection Plan; (7) Regional Transportation Security Strategies; and (8) Transportation Sector Specific Plan.



CHAPTER 6: FIGURE 53: Categories of the NPA 33

Source: Department of Homeland Security in the 2007 Transit Security Grant Program (TSGP)

HOMELAND SECURITY

The National Response Framework (formerly the National Response Plan), identifies the key personnel, roles, responsibilities and mechanisms for the Nation's response to incidents. The lead federal agency for ESF#1 is the U.S. Department of Transportation. DOT is responsible for planning and coordination of activities affecting transportation throughout all incident areas – prevention, preparedness, response, recovery and mitigation.

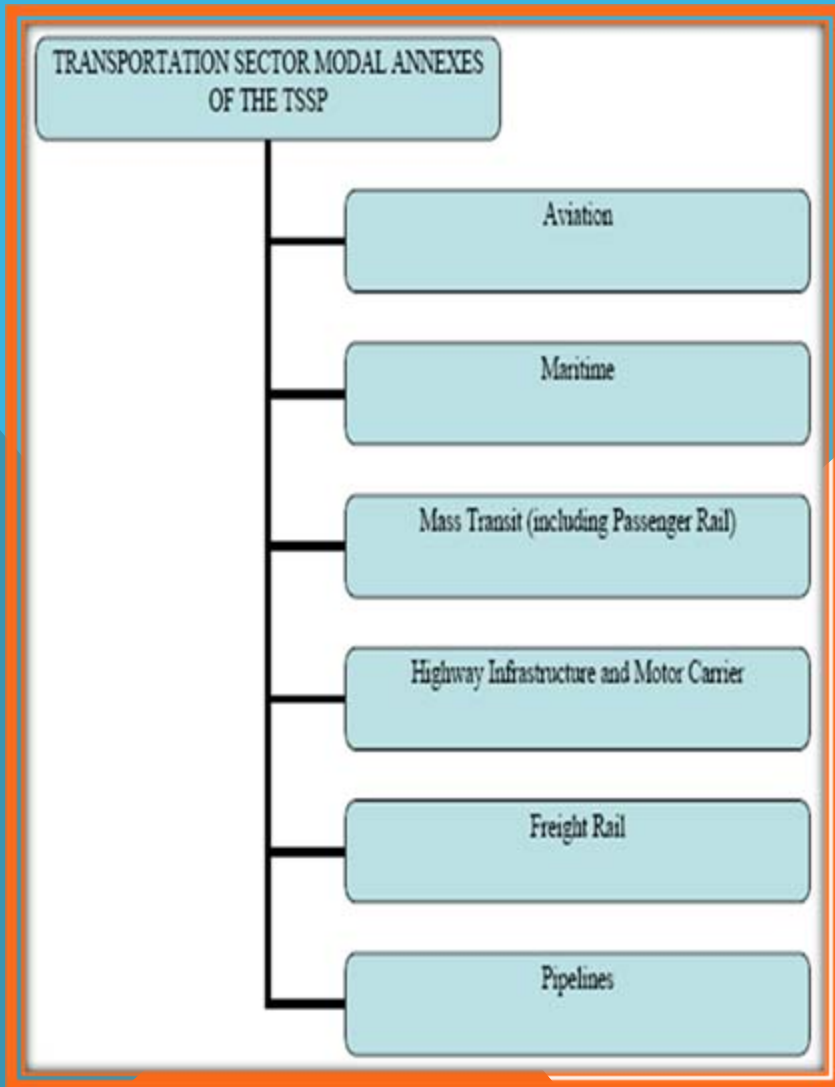
ESF #	Function
1	Transportation
2	Communications
3	Public Works and Engineering
4	Firefighting
5	Emergency Management
6	Mass Care, Emergency Assistance, Housing, and Human Services
7	Logistics Management and Resource Support
8	Public Health and Medical Services
9	Search and Rescue
10	Oil and Hazardous Materials Response
11	Agriculture and Natural Resources
12	Energy
13	Public Safety and Security
14	Long-Term Community Recovery
15	External Affairs

CHAPTER 6: FIGURE 54: Emergency Support Functions

Source: Adapted from National Response Framework (NRF), National Infrastructure Response Plan (NIPP), Jan 2008)

HOMELAND SECURITY

Transportation Sector Specific Plan (TSSP)



Perhaps the most significant NPA component for purposes of transportation agency security is the Sector Specific Plan. It is known formally as the Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (TSSP), published by DHS in May 2007. The main body of the TSSSP document contains significant detailed information about issues associated with the transportation sector.

CHAPTER 6: FIGURE 58: Transportation Sector Modal Annexes of the TSSP

Source: Adapted from Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan, 2007

Overview of the Appendices

APPENDIX A

Thirty-one (31) pages of annotated references with information provided regarding how or where to acquire copies of the material.



APPENDIX B

Over one hundred (100) more references including additional source information.

Overview of the Appendices

APPENDIX C

APPENDIX D

A listing of over
one thousand
(1000) Security
Related
Acronyms and
Abbreviations

CBS	Central Broadcasting System
CBWNP	Chemical and biological weapons nonproliferation program
CC	Cable Car
CCA	Contamination Control Area
CCB	Construction Criteria Base
CCE	Certified Cost Engineer
CCP	Casualty Collection Point
CCRF	Commissioned Corps Readiness Force (part of PHS)
CCTV	Closed Circuit Television
CCV	Characteristics and Common Vulnerabilities
CCVE	Closed-Circuit Video Equipment
CDC	Centers for Disease Control and Prevention (part of HHS)
CDISS	Centre for Defense and International Security Studies
CDL	Commercial Drivers License
CDLIS	Commercial Driver's License Information System
CDP	Center For Domestic Preparedness
CDRG	Catastrophic Disaster Response Group
CEMP	Certified Emergency Management Plan
CEO	Chief Executive Officer
CEQ	Council on Environmental Quality
CERC	Crisis and Emergency Risk Communications
CESB	Council of Engineering and Scientific Specialty Boards
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulations
CFSAN	Center for Food Safety and Applied Nutrition (part of FDA)
CG	Phosgene
CI/KR	Critical Infrastructure/Key Resource
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CIBADS	Canadian Integrated Biological Agent Detection System
CIP	Critical Infrastructure Protection

A listing of over
one thousand
(1000) Security
Related Terms and
Definitions

NCHRP PROJECT 20-59(28)

SECURITY 101: A PHYSICAL SECURITY PRIMER FOR TRANSPORTATION AGENCIES

Presentation to

*Transportation Hazards & Security
Summit and Workshop 2010*

Wednesday, August 25, 2010

Beckman Center of the National Academy
of Sciences and Engineering Irvine,
California



*Countermeasures Assessment &
Security Experts, LLC*

110 Quigley Boulevard

Airport Park

New Castle, DE 19720

302-322-9600