PARTICIPANT GUIDE

U.S. Department
of Transportation

**Federal Transit
Administration**

TRANSIT SYSTEM SECURITY PLANNING SEMINAR

Prepared by:
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
Safety and Security Systems Division
Cambridge, Massachusetts 02142

Prepared for:
Federal Transit Administration
Office of Safety and Security
Washington, DC 20590

June 1996

FTA OFFICE OF SAFETY AND SECURITY

AHA!!!

(Ideas for Action)

Quite often, when participating in training or other group sessions, ideas may arise that prompt you to say, "AHA, I OUGHT TO DO THAT!". Experience has taught that we tend to forget and not use those ideas if we wait more than 24 hours or don't deposit them in a place where they will be available to us. For this reason, we have created the area below for you to jot down those ideas and/or actions (i.e., things that you can take back with you) to do when you return to your home organization.

"To accept good advice is but to increase one's own ability."
Goethe

Table of Contents

Introduction *Module 1*

Summary
Module 1 outlines the seminar objectives along with the knowledge and skills to be acquired by the students.

1. Seminar objectives

Upon successful completion of this seminar, the student will have acquired the following knowledge and skills.

Knowledge:	**Skills:**
1. Understanding the concept of System Security.	1. Application of System Security to the mass transit environment.
2. Understanding the elements of a dynamic System Security Program and application of systematic approach to identify threats and vulnerabilities.	2. Implementation of a successful System Security Program.
3. Understand the threat and vulnerability resolution process.	3. Application of techniques used to identify threats and vulnerabilities and methods used to resolve them.

2. How to use your seminar outline

This seminar outline will assist you in learning the concept and application of security program management. It is intended for your personal use; after you complete the outline, it and and the handouts can be used by you as a reference.

3. Presentation of material

The seminar material is in outline form. It is necessary that you take notes to complete various items. As with any instruction, the effectiveness of this seminar depends upon your active participation in the seminar dicussion and exercise.

What is Transit Security? *Module 2*

Summary
Module 2 introduces the concepts of Security, Transit Security, and System Security. The proactive nature of System Security is detailed as well as its utility over the life cycle of a system. Finally, the concepts of Risk, Threat, and Vulnerability are introduced.

1. What is transit security?

a. Freedom from intentional danger
- Passengers
- Employees
- System

OPEN DISCUSSION: IDENTIFYING SECURITY ISSUES
Identify security issues that face transit systems and the environment in which they operate

2. How security is measured: the importance of perceived security vs. actual security

a. *Perceived* security is as important to a transit agency as actual security performance

- Patron fear reduces ridership and heightens the anxiety of passengers, even though most transit systems are many times more secure than the neighborhoods in which they operate

- Security is communicated to patrons not only by the actual security performance of the system, but also by the perceptions patrons form about the system

b. Security is measured by patrons in terms of perception

- Patrons make decisions regarding the security of a system based largely upon their own assessments

- Patrons perceive security in the following ways:

  - Direct sensory experience (lighting, cleanliness, graffiti, vagrancy, etc.)
  - Personal knowledge of security incidents (being victimized on the system)
  - Published accounts of transit system security problems (media coverage)
  - Reported experiences of others (relatives and friends who have been victimized on system or witnessed others being victimized)

3. ***A security program must address both perceived and actual security problems if it is to reassure patrons, maintain or increase ridership, and earn the public trust***

4. ***Common security attitudes***

a. No major security incidents so we must be doing it right.
b. That is remote and anyway it can't happen here.
c. Can't put too much authority in the police or security department.
d. Don't really understand system security or why we need it; they don't do it.
e. If we have an incident we will deal with it then (Tombstone Operations).
f. We are all set as our system is already secure.
g. Security is not my job, its the security officer's.
h. Not doing it is saving money.

5. ***The importance of perception to preventing crime: the theory of Broken Windows***

a. James Q. Wilson and George Kelling hypothesis -- Quality-of-life crimes, such as vandalism and destruction of property, lead to more serious crimes by reducing order, encouraging both offenders and citizens to believe that lawlessness is tolerated

b. Wilson/Kelling recommendation: Place a high priority on activities that increase the perception of security

6. *Actual Security: Categories of intentional harm*

a. FBI Uniform Crime Reporting Program and Classification System

- Established in 1930, the UCR Program collects statistics to document the crime problem in America from over 16,000 Federal, state, and local law enforcement agencies. Data collected for the UCR program is submitted according to policies and procedures outlined by the FBI in the Uniform Crime Reporting Handbook. The Handbook ensures the best reporting possible by taking law enforcement agencies through data coding processes that improve the reliability of crime statistics. For more information on this program, please write to:

  Uniform Crime Reports
  Federal Bureau of Investigation
  Washington, D.C. 20535

- FBI efforts to develop the National Incident-Based Reporting System (NIBRS), and the planned shift from Part I and Part II Crimes to Group A and Group B Offenses

- Transit agencies report transit crime as part of the National Transit Database. The reporting categories are consistent with the UCR. The statistics will be available through the Safety Management Information Statistics (SAMIS) Annual Report.

b. Strengths and weaknesses of the UCR program for transit crime statistics

- Utility of the FBI UCR Program to support local data analysis efforts
  - Ability to identify nation-wide trends: when and where crime takes place, what form it takes, and the characteristics of its victims and its perpetrators
  - Availability of data from all levels of law enforcement
- Limitations of UCR data for transit systems
  - Transit police often report their crime to the local/municipality police to be reported to the State and FBI UCR programs. Thus, transit crime data is folded into city/county/municipality data

- Local police who respond to transit incidents may not code the incidents as being transit-related.

c. Part I Crimes

- Arson
- Burglary
- Homicide
- Motor Vehicle Theft
- Rape (forcible and attempted)
- Robbery (weapon and strong arm)
- Theft (pickpocket, purse-snatch, automobile burglary, automobile accessories, bicycle, computer fraud, vending machine fraud)

d. Part II Crimes

- Bomb Threats
- Drunk Driving
- Drunkeness
- Gambling
- Kidnapping
- Liquor Law Violations
- Narcotics
- Sex Offenses Excluding Rape (indecent exposure and other)
- Trespassing
- Vagrancy
- Vandalism
- Weapon Law Violations

e. Local Offenses (enforced by municipal code/state law/transit adjudication board)

- Fare Evasion
- Loud Music
- Public Expectoration/Urination
- Rowdy Behavior
- Smoking, Eating, Drinking on the System

f. Terrorism
   - A criminal act committed against society to receive attention for a political or personal motive. Often these acts are violent and involve multiple injuries and considerable property damage.
     - Assassination
     - Bombings
     - Sabotage

7. Social costs of transit crime

a. Personal harm to victims

b. Poor perception of security

c. Congestion outside the system

d. Reduced quality of life on system

8. Financial costs of transit crime

a. Increased financial burden of operating the system
   - Repairs
   - Liability/compensation to victims
   - Schedule disruptions
   - Law enforcement
   - Security equipment

b. Reduction of revenues collected
   - Internal theft
   - Lost ridership
   - Fare evasion

9. ***Why security is important in the nineties***

a. Renewed emphasis on mass transit to resolve urban congestion

b. Increase in security-related costs
- Reduced ridership (poor patron perception)
- Lower employee morale
- Higher cost of claims against system
- Higher cost of security/police
- Higher cost of transferring risk (insurance premiums)
- Higher cost of replacing service interrupted by incidents
- Higher cost of equipment/system repairs (vandalism)

c. Federal and local policies emphasizing security (i.e., State Safety Oversight, FTA 1 percent security set aside, ISTEA, community task forces and community policing)

d. Improved security technologies

Summary

Module 3 provides an overview of the State Safety Oversight Rule (the Rule). It also outlines the impact the Rule has on the security operations of transit agencies who operate rail fixed guideway systems.

1. Why have a State Safety Oversight Rule?

a. Intermodal Surface Transportation Efficiency Act of 1991
- Section 28 to Federal Transit Act 49 U.S.C. 5330
- Requires FTA to issue regulations creating a state oversight program
- 49 CFR 659 is the final rule for the State Safety Oversight Program

2. An overview of the Rule

a. The designation of a state safety oversight agency
- The responsibilities of the state safety oversight agency
- The responsibilities of the rail fixed guideway system
- The consequences of non-compliance
- Rule is effective as of January 26, 1996

3. General provisions of the Rule

a. Requires the state to oversee the safety of rail fixed guideway systems
- Applies to all rail fixed guideway systems not regulated by the FRA

b. Provides definitions for terms accident, safety, security, etc.

c. Authorizes withholding of funds for non-compliance

4. Definition of a rail fixed guideway system

"Any light, heavy or rapid rail system, monorail, inclined plane, funicular, trolley, or automated guideway that is included in FTA's calculation of fixed guideway route miles or receives funding under FTA's formula program for urbanized areas and is not regulated by the Federal Railroad Administration."

5. ***The role of the state***

   a. Identify and designate an oversight agency
      - Certify oversight agency to FTA

   b. Provide for confidentiality of investigation reports

   c. Prevent public disclosure of security portion of SSPP

6. ***The role of the oversight agency***

   a. Develop the system safety program standard

   b. Require and approve transit agency system safety program plans

   c. Require the transit agency to submit an annual safety audit report

   d. Conduct on-site safety reviews every three years

   e. Conduct investigations

   f. Require transit agencies to prepare corrective action plans

   g. Submit of reports to the FTA

   h. Monitor transit agency use of contractors

   i. Issue transit agency certification of compliance

7. ***The system safety program standard***

   a. APTA Manual for Development of Rail Transit System Safety Guidelines
      - APTA guidelines are the minimum standard
      - Agencies using MIL-STD-882 should meet if not exceed the APTA standard
      - Must be implemented by January 1, 1997

   b. Address the personal security of passengers and employees (new requirement)
      - Must be Implemented by January 1, 1998

8. ***Oversight agency on-site reviews***

a. Conduct safety reviews every three years

b. Purpose
- Encourage oversight agency to maintain proactive role
- Allow oversight agency to address system safety and security issues

c. Review of Transit Agencies Implementation of System Safety Program

d. Prepare and issue a report containing:
- Findings and recommendations
- Analysis of adequacy of System Safety Program Plan
- Determination of whether it should be updated

9. ***Oversight agency investigations***

a. Establish procedures to investigate accidents and unacceptable hazardous conditions

b. Investigate accidents and unacceptable hazardous conditions unless the National Transportation Safety Board is investigating

10. ***Corrective action plans***

a. Oversight agency must require the transit agency to minimize, control, correct, or eliminate any investigated hazardous condition

b. Oversight agency must require transit agency to develop a corrective action plan

c. Corrective action plan must specify time period by which hazardous condition will be resolved

11. ***Submission of reports to the FTA***

a. Initial submissions

b. Annual submissions

c. Periodic submissions

12. An oversight agency may use contractors to perform the following activities

a. Develop a system safety program standard

b. Review system safety program plans

c. Review annual audit reports

d. Conduct safety reviews

e. Prepare safety review findings

f. Establish investigation procedures

g. Conduct investigations

h. Review corrective action plans

i. Prepare initial or annual submissions to FTA

13. Certification of compliance

a. Oversight agency must certify to FTA before January 1, 1997 that it has complied with each part of the rule

b. Oversight agency must thereafter certify to FTA annually that it has complied with each part of the rule

c. Certification shall comply with the sample certification provided in the appendix the rule

14. The role of the transit agency operating a rail fixed guideway system

a. Prepare and submit a system safety program plan that meets the standard

b. Conduct safety audit and submit annual reports

c. Classify hazardous conditions

d. Report accidents and unacceptable hazardous conditions report to oversight agency

e. Prepare and submit corrective action plans

f. Maintain communications with oversight agency

15. ***The oversight agency may allow a transit agency to use contractors for the following activities***

a. Develop or update a system safety program plan

b. Prepare annual audit reports

c. Develop a corrective action plan.

16. ***Annual safety audits by the transit agency***

a. Checklist 9 of APTA guidelines requires a report summarizing findings of internal safety audit

b. Require transit agency submit to oversight agency a copy of the report on the annual safety audits

c. Oversight agency review of annual audits

17. ***The role of the FTA***

a. Issue the Rule

b. Assess adequacy of state efforts to comply with the Rule

c. Analyze reports submitted by oversight agencies

d. Assist states in implementing rule

1. What is System Security?

Definition	
SYSTEM	A system contains four elements: people, equipment and facilities, procedures, and environment
SYSTEM SECURITY	The proactive application of operating and management principles to reduce the security vulnerabilities of a transit system to the lowest level practical

2. System security and the system life cycle

Security issues are considered in a system's:

a. Planning

b. Design

c. Construction

d. Operation

3. Characteristics of a System Security approach

a. Pro-active and concentrates resources on crime prevention

- Environmental design is emphasized
- Data collection, analysis, and monitoring are primary means of maintaining security

b. Uses both theoretical and practical means of analysis

c. Gives equal priority to the security of passengers and employees

d. Maintains attitude that many crimes are preventable

4. System Security approach relies on risk, threat, and vulnerability management

Definition
RISK Probability that a security incident will occur **THREAT** Any real or potential condition that can result in a security incident **VULNERABILITY** Any condition or act that endangers human life or property

Summary

Module 3 introduces the System Security Program as well as its benefits and requirements. Four issues are discussed:

- *The Purpose of a System Security Program*
- *The Requirements of a System Security Program*
- *What a System Security Program Can Do for Your Security/Police Department*
- *The Implementation of a System Security Program*

1. What is a System Security Program?

Definition

SYSTEM SECURITY PROGRAM

A form of risk management that eliminates or controls transit system threats and vulnerabilities through an ongoing threat and vulnerability resolution process

2. Purpose of a System Security Program

a. Identify system threats and vulnerabilities

b. Determine risk level acceptable to management

c. Eliminate or manage threats and vulnerabilities

d. Evaluate effectiveness of program

3. ***A System Security Program does not require:***

   a. An increase in the size of security/police department

   b. An increase in the budget of the security/police department

   c. An increased amount of security equipment

4. ***To be effective, a System Security Program does require:***

   a. An increase in the visibility of the security/police department at the system

   b. Increased input from the security/police department in system decision making

   c. An increase in the security responsibilities assumed by other departments

   d. An increased efficiency in the ways in which the security/police department expends resources

5. ***How a System Security Program may differ from your security/police department's existing security activities:***

   a. Focuses on using the system environment to prevent crimes, rather than focusing exclusively on response to the crimes that occur

   b. Includes all transit departments, not only those specifically charged with security

   c. Relies heavily on data collection and analysis to assess performance, identify problems, and design appropriate countermeasures

   d. Manages security activities through the use of thorough documentation and interagency cooperation

   e. Requires access to and the support of top management

6. *How to implement a System Security Program: a six-step process*

a. Obtain management support for the program

b. Assess current security activities/responsibilities of all transit departments

c. Develop and document the program in the program plan

d. Obtain top management approval for the program plan

e. Develop threat and vulnerability resolution process

e. Follow-up

7. *System Security Program Contents*

A system security program can provide transit system patrons and employees with the highest degree of security practical only if it is documented in a system security program plan, and it does the following:

a. Includes both patrons and employees.

b. Addresses all organizations within the transit system.

c. Provides for and maintains top management approval in the form of a signed policy and the allocation of adequate resources.

d. Establishes a proactive security program with the process and procedures necessary to identify and resolve threats and vulnerabilities before they result in security incidents.

e. Addresses all the security issues associated with the transit system.

f. Designates one individual as the security authority for the system and ensures direct access to the general manager.

g. Clearly identifies the roles and responsibilities of the security director/officer and the security department.

h. Clearly identifies the security roles and responsibilities of all other transit departments.

i. Includes a mechanism that requires security as a goal for all employees.

j. Provides a mechanism for cooperation between the individual transit system departments and external agencies that support the system.

k. Includes review of databases to assist in the continuous monitoring of the system security program and to assure that it is providing the expected results.

8. System Security Program Elements

In order to be successfully implemented, a system security program plan must contain the following three elements.

a. Management commitment to the program
- Policy
- Resources
- Responsibilities

b. Application of system security throughout the system life-cycle
- Threat and vulnerability management in acquisition phase
- Threat and vulnerability management in operational phase

c. Plan to implement and document the program
- Management commitment
- System security tasks
- Schedule for program implementation and maintenance

Obtain Management Support for the System Security Program

Module 6

1. ***Obtain management Support for the System Security Program***

   a. Because a System Security program requires procedural changes in the way transit agency departments relate to each other, management support is essential

   b. While top management approval will be needed for each document that formally implements the System Security program, a Chief Executive Officer's Policy Statement is an important first step

2. ***Chief Executive Officer's Policy Statement***

   a. Emphasizes importance of security

   b. Designates Security/Police Department responsibility

   c. Establishes authority of Security/Police Department

   d. Demonstrates management commitment of resources and personnel

   e. Should be widely distributed

SAMPLE POLICY STATEMENT

Memorandum

To: **All employees and other interested individuals**
From: **(General Manager or Executive Director)**
Date:
Re: **System Security Policy**

The _____ was created to provide safe, secure, and reliable service to its passengers. To this end, it is the responsibility of each and every _____ employee to ensure the security of passengers, employees, system property.

The _____ is authorized and directed to develop, implement, and administer a comprehensive and coordinated System Security Plan to prevent incidents from occuring , and resolving those that may occur.

It is the responsibility of each _____ employee to cooperate with _____ and provide him with any requested infiormation to assist in any investigation or inspection that he may undertake.

3. Real Honest Commitment

a. Acceptance by top management of security responsibility. Make top management accountable to the board of directors.

b. Identify the security responsibility of everyone.

c. Understand that security can increase ridership/revenue.

d. Make security an element of performance appraisals.

e. Designate a security person with the authority to _____.

f. Give security equal ranking with other considerations in the selection of all projects.

g. Establish strong security monitoring and enforcement program.

WORKSHOP: VIEWGRAPH EXERCISE

Use the viewgraph you have been given to draw an organization chart showing how a police/security organization would fit into a transit agency, and how the organization would report to management. Choose someone in your group to present your organization chart to the class. Be prepared to discuss the pros and cons of your choice.

4. Presenting System Security to management

a. Introduction

- Why you are there
- How much time you will use
- What you want

b. Define system security

c. Provide justification for a system security program

d. State objective of proposed system security program

e. Explain benefits

f. Describe approach

g. Explain resources needed
- Time
- Cost
- Materials
- Personnel
- Space

h. Ask for commitment

i. Closure

ROLE PLAY: SELLING SYSTEM SECURITY TO MANAGEMENT

Break into groups. Assign one person as General Manager, another person to sell the concept of System Security to the General Manager. The roles the rest of your group may play are up to your imagination. Be prepared to act out a meeting where a transit employee sells the concept of System Security to the General Manager.

Determine all Transit System Security Responsibilities

Module 7

1. ***Who is Responsible for Security?***

   a. Security/Police Department

   b. Other transit departments

   c. Patrons

2. ***Security/Police Department responsibilities***

   a. Assess current security/police department responsibilities

      - Inventory current security personnel and functions
      - Identify all security activities performed by the security/police department
      - Assess data collection/processing activities
      - Review training/recruitment activities

   b. Identify security activities of other transit system departments

      - Identify crucial security functions performed by other departments (i.e. maintenance -- lighting, operations -- keys/passes for authorized areas, etc.)

      - Assess data collected by other departments that would assist the security/police department in designing programs/countermeasures

      - Identify contact people within each department

c. Identify security roles of outside organizations

- Local police
- Emergency response organizations
- Other transportation systems (transit agencies, traffic control groups)
- Security watch-groups (community neighborhood watch, etc.)
- Media
- Federal, state, and local governments
- Utilities (water, gas, and electricity)
- Planning authorities and commissions
- Schools

d. Design the System Security Program

e. Document the System Security Program in a System Security Program Plan

- Include a list of specific security tasks for each position

f. Manage and evaluate the System Security Program

3. Other Transit Department Responsibilities

a. Understand security's role in system operation

b. Summarize security responsibilities of all departments

c. Establish joint committees with Security/Police Department to address security issues

4. Patron Responsibilities

a. Information

b. Behavior modification

c. Community organizations

WORKSHOP: LIST SECURITY RESPONSIBILITIES OF FOLLOWING DEPARTMENTS
Engineering Finance Human resources Line supervisors Maintenance Management staff Operations Safety Training Policy and Planning Audit Union Legal General Manager / CEO Public Affairs

WORKSHOP: LIST SECURITY RESPONSIBILITIES (Continued)

Security responsibilities of _____

-

-

-

-

-

Security responsibilities of _____

-

-

-

-

-

Security responsibilities of _____

-

-

-

-

-

WORKSHOP: LIST SECURITY RESPONSIBILITIES (Continued)

Security responsibilities of _____

-

-

-

-

-

Security responsibilities of _____

-

-

-

-

-

Security responsibilities of _____

-

-

-

-

-

WORKSHOP: LIST SECURITY RESPONSIBILITIES OF TRANSIT POLICE / SECURITY ORGANIZATION
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.

Develop and Document the Program in the Program Plan

Module 8

1. What is a System Security Program Plan?

Definition
SYSTEM SECURITY PROGRAM PLAN The formal document that describes the planned security tasks required to meet the System Security requirements. It outlines organizational responsibilities, levels of commitment, methods of accomplishment, scheduling milestones, depth of effort, and integration with other design and management activities.

2. The SYSTEM SECURITY PROGRAM is documented in the Program Plan

3. Relationship between the Program and the Program Plan

The System Security Program and the System Security Program Plan will identify, document, and manage the ways in which the security/police department, other departments, and patrons are responsible for security

4. A Program Plan does the following:

a. Describes an integrated effort within the transit system among management, the Security/Police Department, and all other departments

b. Specifies the management review process and the Security/Police Department role during system design, modification, and development

c. Identifies all System Security goals, objectives, and requirements

d. Describes the method of conducting System Security analyses, collecting information, and reporting results

e. Identifies any unusual security activities that must be performed as a result of technology, procedural necessity or information collection requirements

f. Summarizes the program activities necessary to complete the System Security goals, objectives, and requirements

g. Details content of security training program, schedule of training, and level of training required for each position

5. ***The Program Plan manages the Program***

The Program Plan clarifies the following Program objectives:

a. Mission statement

b. Security objectives/goal setting based upon management commitment

c. Tasks essential to achieve security objectives

d. Organizations that will perform the security tasks and subtasks

e. Interfaces between Security/Police Department and other organizations (internal and external)

f. Informational needs (which data must be gathered; how data should be maintained; which technical analyses should be applied)

g. Necessary informational outputs (reports, inspections, follow-ups, and reviews)

h. Scheduling security efforts

6. ***The Program Plan management activities***

a. Ultimate responsibility for secure transit system operations

b. Communication of security as top management priority

c. Development of relations without outside organizations that contribute to security program

d. Proactive identification of security concerns

e. Solicitation of security concerns of other employees

f. Commitment to ensure that the Program is carried out on a daily basis

7. ***The Program Plan should address the following activities***:

a. Interface with internal/external organizations/review committees

b. Collect and review security data

c. Conduct audits and investigations

d. Identify and resolve security issues

e. Implement security awards and incentives program

f. Review specifications for procurement

g. Perform training

h. Assist other organizations in carrying out security activities

8. ***Suggested Contents of a Program Plan***

a. Overview of system security

- Purpose and scope of the security program and program plan

b. Description of transit system

- Background and history of system
- Organizational structure
- Existing security capabilities
  - Proactive measures
  - Response measures
- Existing security concerns

c. Description of how program plan will be managed

- Mission statement
- System security policy
- Security responsibilities
- Review committees

d. Security Roles and Responsibilities

- Planning
- Proactive measures
- As a deterrent - providing a presence
- Training
- Day-to-day activities
- Non-emergency requests (information, etc.)

e. Threat and vulnerability identification, assessment, and resolution

- Threat and vulnerability identification
  - Security inspections
  - Data collection
  - Reports
  - Security information flow

- Threat and vulnerability assessment
  - Responsibility
  - Data analysis
  - Frequency and severity

- Threat and vulnerability resolution
  - Emergency response
  - Incident investigation
  - Research countermeasures
  - Make decision to eliminate, control, or accept threat/vulnerability

f. Implementation of the Program Plan

- Goals and objectives (establish performance measures)
- Schedule
- Program implementation (programs that affect measures)
- Evaluation of performance measures
  - Internal review
  - External review

g. Modification of the Program Plan

- Initiation
- Review process
- Implement modifications

h. Periodic review and update of Program Plan

9. System Security Program Assessment

a. Internal program audit / review

- Is there a published and widely distributed Security Directive (Policy Statement) from the Chief Executive Officer (CEO)?
  - Does the directive define or describe management security goals or requirements?
  - Does the directive define organized security responsibilities and authority?
  - Does the directive require or implement a documented security program? Why? Alternative?
  - Has the directive been issued or concurred in by the current CEO?

- Is there a formal System Security Program Plan? If so:
  - Is it up to date?
  - Is it widely distributed?
  - Is it being used?

- Is the Police/Security Department effective?
  - Does it provide input to plans and specifications?
  - Does it concentrate on preventive rather than remedial security?
  - Are its investigations primarily aimed at future prevention rather than fixing blame?
  - Are its recommendations welcomed and acted upon?

- Do other departments fulfill their security responsibilities?
  - Are new employees indoctrinated in security?
  - Do managers accept their responsibility for security?
  - Is security talked about before an incident, or only afterwards?

b. External reviews

- FTA
- FRA
- IACP
- APTA
- State and local government
- Peers (other transit systems)

10. Other system documents requiring security input

a. System policies (security and other)

b. System procedures (security and other)

c. System analyses (threats and vulnerabilities, financial, fault tree)

d. Management reporting documents

e. Rule books/operating procedures

f. Maintenance procedures

g. Training

h. Inspection procedures

i. Design specifications and drawings

j. Emergency procedures

k. Inter-agency organization agreements

l. Surveys

m. Audits

n. Audit/inspection reports

o. Incident investigations

p. Public information

11. Obtain Top Management approval for the System Security Program Plan

a. Signed system security program plan

b. Management participation in interdepartmental cooperative efforts

c. Management cover letter for the distribution of the system security program plan

Definition
THREAT AND VULNERABILITY ANALYSIS The comprehensive study of a system to identify threats and vulnerabilities and to make recommendations for their elimination or control during all life cycle phases.

1. ***A threat and vulnerability resolution process outlines how actual and potential threats will be identified, evaluated, and resolved. Proper threat identification, categorization, and data collection are crucial to this process.***

2. ***Elements of a threat and vulnerability analysis***

   a. Define the system

   b. Identify threats and vulnerabilities

   c. Assess threats and vulnerabilities

   d. Perform threat and vulnerability reduction precedence

   e. Resolve threats and vulnerabilities

   f. Follow up

3. ***Threat and vulnerability identification aids***

   a. Formal threat and vulnerability analysis

   b. Expert opinion

   c. Scenarios

   d. Checklists

   e. Data

4. ***Pre-incident indicators***

   a. Theft

   b. Local unemployment

   c. Area demographics

   d. Proximity of junior/senior high schools

   e. Proximity of entertainment areas (e.g., sports arenas)

5. ***Types of threat and vulnerability analyses***

   a. INDUCTIVE

      An analysis to determine the effect of specific events. (A bottom up approach - what happens if a specific event occurs.)

   b. DEDUCTIVE

      An analysis of a specific event to determine possible causes of that event. (A top down approach - what can cause a specific event to occur.)

6. ***Typical types of threats and vulnerabilities***

   a. Altered, depleted, or removed security devices

   b. Unauthorized changes to equipment or procedures

   c. Equipment used for unintended purposes

   d. Unauthorized use of equipment

   e. Improper procedures

   f. Inoperative equipment

   g. Inadequate procedures

   h. Inadequately designed equipment/facilities

   i. Other unsecure conditions or acts

6. *Threat severity categories*

Category	Severity	Characteristics
1	Catastrophic	Death or system loss
2	Critical	Severe injury, severe occupational illness or major system damage
3	Marginal	Minor injury, minor occupational illness or minor system damage
4	Negligible	Less than minor injury, occupational illness or system damage

Reference MIL-STD-882C

7. *Vulnerability probability categories*

Description *	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to ocur, but possible

Reference MIL-STD-882C

* Definitions of descriptive words may have to be modified based on quantity involved

** The size of the fleet or inventory should be defined

8. *Threat and vulnerability assessment matrix*

Frequency of Occurence	Vulnerability Categories			
	Catastrophic	Critical	Marginal	Negligible
Frequent	1A	2A	3A	4A
Probable	1B	2B	3B	4B
Occasional	1C	2C	3C	4C
Remote	1D	2D	3D	4D
Improbable	1E	2E	3E	4E

Unacceptable
Unacceptable (Management decision required)
Acceptable with review by management
Acceptable without review

Reference MIL-STD-882C

9. *Threat and vulnerability reduction precedence*

a. Design to eliminate

b. Design to control

c. Security devices

d. Warning devices

e. Special procedures

f. Accept

10. *Factors influencing the threat and vulnerability resolution process*

a. Technological considerations

b. Time considerations

c. Relative effectiveness

d. Impact on operations

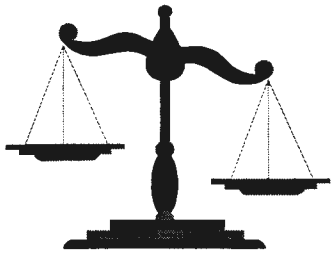
e. Economic considerations (equipment and labor)

f. Political considerations

11. Trade offs of threat and vulnerability management

Threat and vulnerability

- Probability of occurrence
- Severity



Controls

- Design to eliminate the threat or vulnerability
- Design to control the threat or vulnerability
- Add security devices
- Add warning devices
- Institute special procedures or training

WORKSHOP: SECURITY CONSIDERATIONS IN ACQUISITION

1. Vehicle Design

   -

   -

   -

   -

2. People

   -

   -

   -

   -

3. Procedures

   -

   -

   -

   -

4. Environment

   -

   -

   -

   -

Outline for a System Security Program Plan *Appendix A*

Title Page
Acknowledgements
Table of Contents
Foreword
Management Commitment and Directive/Policy
Executive Summary

I Introduction to System Security
- a. Purpose of System Security Program Plan and Program
- b. Goal, Objectives, and Tasks of the Program
- c. Scope of Program
- d. Security and Law Enforcement
- e. Management Authority and Legal Aspects
- f. Government Involvement
- g. Definitions within the System Security Program Plan

II Transit System Description
- a. Background and History of Transit Agency
- b. Organizational Structure
- c. Human Resources
- d. Passengers
- e. Transit Services / Operations
- f. Operating Environment
- g. Facilities and Equipment
- h. Passenger, Vehicle, and System Safety Plan and Program
- i. Current Security Conditions
- j. Existing Security Capabilities and Practices

III Management of the System Security Plan
- a. Responsibility for Mission Statement and System Security Policy
- b. Management of the Program
- c. Division of Security Responsibilities
- d. Proactive Security Committee
- e. Security Breach Review Committee

IV System Security Program: Roles and Resposibilities
- a. Planning
- b. Proactive Measures
- c. Training
- d. Day-to-Day Activities

V Threat and Vulnerability Identification, Assessment, and Resolution
  a. Threat and Vulnerability Identification
    - Security Testing and Inspections
    - Data Collection
    - Reports
    - Security Information Flow
  b. Threat and Vulnerability Assessment
    - Responsibility
    - Data Analysis
    - Frequency and Severity
  c. Threat and Vulnerability Resolution
    - Emergency Response
    - Breach Investigation
    - Research and Improvements
    - Eliminate, Mitigate, or Accept

VI Implementation and Evaluation of System Security Program Plan
  a. Implementation Goals and Objectives
  b. Implementation Schedule
  c. Evaluation
    - Internal Review - Management
    - External Audits

VII Modification of the System Security Plan
  a. Initiation
  b. Review Process
  c. Implement Modifications

Appendix A. Bibliography

Appendix B. Glossary of Security Terms

Appendix C. Security-Related Boards, Panels, Committees, Task Forces, and Organizations

Appendix D. Security Forms and Logs

Additional Appendices

WORKSHOP: DEVELOPING A SYSTEM SECURITY PROGRAM

Forest Hills Transit Authority (FHTA) is a medium-sized bus system in the South that serves the Forest Hills City area and surrounding suburbs. The system operates approximately 20 routes between 6:00am and 11:00pm during weekdays and for restricted hours on weekends.

In 1983, a significant increase in serious crimes on the system caused the FHTA Board to create the FHTA Security Department to protect patrons, employees, and system assets. Employing ten (10) non-sworn security guards, the FHTA Security Department patrols bus stations, parking lots, building facilities, and the FHTA offices. The Department also records data on the security incidents that occur on the system.

During the decade since its inception, the Security Department has worked diligently to reduce crime on the system. However, while focusing on security concerns, the Department has not devoted time to building relationships with other FHTA Departments. Recently, the Department's relations with Operations have become strained, because the operators do not believe that the Security Department is doing all it can to prevent/respond to the incidents that occur on their buses.

While the Security Department does not communicate much with other FHTA departments, it has forged a close relationship with the Forest Hills City Police, who, until recently, responded to most system incidents. However, budget cuts have reduced the ability of the Forest Hills Police to assist the FHTA Security Department. The Forest Hills Police have made it clear that they can only respond to serious incidents on the system, and will no longer be available to assist the FHTA Security Department with minor incidents, such as drunken/disorderly and vandalism cases.

Unfortunately, as experienced by FHTA's bus operators, a significant increase in these types of incidents has occurred. The Security Department now must devise a strategy to limit their occurrences. Working with your team, use the information listed below to develop a System Security Program to help the FHTA Security Department reduce crime on its system.

FHTA Information Sheet

1) Summary of FHTA Transit Crime Statistics

1993				1983		
1993 Total Ridership	1993 Total Incidents of Crime	1993 Part I Offenses	1993 Part II Offenses	1983 Total Incidents of Crime	1983 Part I Offenses	1983 Part II Offenses
7,000,000	**600**	**55**	**545**	**300**	**65**	**235**

2) Current FHTA Security Department Responsibilities

1. Patrol of System Facilities, Stations, Yards, and Parking Lots
2. Transit Crime Record-keeping
3. Media Relations
4. Cooperation with Forest Hills City Police on Transit Crime Cases

3) Location of Criminal Incidents on the FHTA System

Location	Percent of Part I Offenses (murder, assault, motor theft, etc.) (%)	Percent of Part II Offenses (drunken.disorderly, vandalism, etc.) (%)
On-Board Bus	20%	40%
Bus Stops/Stations	25%	15%
Parking Lots	35%	10%
FHTA Bus Yards	0%	25%
FHTA Facilities	0%	10%
FHTA Money Processing Facility	10%	0%
FHTA Office Building	10%	0%

4) Resources of the FHTA Security Department

1) Budget and equipment for its ten member security staff

2) Advertising/marketing budget of $3,000

3) $10,000 in remaining funds earmarked for the FTA 1% security set-aside

4) Communications systems, including 2-way radios and dispatcher tie-ins

5) Media relations

6) Management Information System for tracking transit crime data

BOMB THREAT

A threat issued against the system to discharge an explosive in an area that may result in serious injuries and significant property damage

CONFIGURATION MANAGEMENT

A process to assure that all documentation that describes a system and its various components is current and reflects the actual functional and physical characteristics of the system throughout its life cycle.

CRIME PREVENTION

The anticipation, recognition, and appraisal of a crime and the initiation of some action to keep it from occurring

CRIME

Combination of three factors:

1. The desire of the perpetrator to commit the crime
2. The perpetrator's ability to carry out that desire
3. The opportunity presented by the victim

DESIGN

Physical, social, management, and law enforcement directives that seek to influence interact with the environment

PHYSICAL ENVIRONMENT

Employees, patrons, and other system users and their structural and social surroundings

RISK

Probability that a security incident will occur

SECURITY PROCEDURE

The steps or methods required by the transit agency to implement its security policies

SECURITY POLICY

Statement of the expectations of the transit agency regarding the behavior of its personnel and the operation of its system in the prevention of security incidents

SYSTEM

A system contains four elements: people, equipment and facilities, procedures, and environment

SYSTEM SECURITY

The use of operating and management principles to reduce the security vulnerabilities of a transit system to the lowest level practical

SYSTEM SECURITY PROGRAM

A form of risk management that eliminates or controls transit system threats and vulnerabilities through an ongoing threat and vulnerability resolution process

SYSTEM SECURITY PROGRAM PLAN

The formal document that describes the planned security tasks required to meet the System Security requirements. It will outline organizational responsibilities, levels of commitment, methods of accomplishment, scheduling milestones, depth of effort, and integration with other design and management activities.

TERRORISM

A criminal act committed against society to receive attention for a political or personal motive. Often these acts are violent and involve multiple injuries and considerable property damage.

THREAT AND VULNERABILITY ANALYSIS

The comprehensive study of a system to identify threats and vulnerabilities and to make recommendations for their elimination or control during all life cycle phases.

THREAT

Any real or potential condition that can result in a security incident

VULNERABILITY

Any condition or act that endangers human life or property