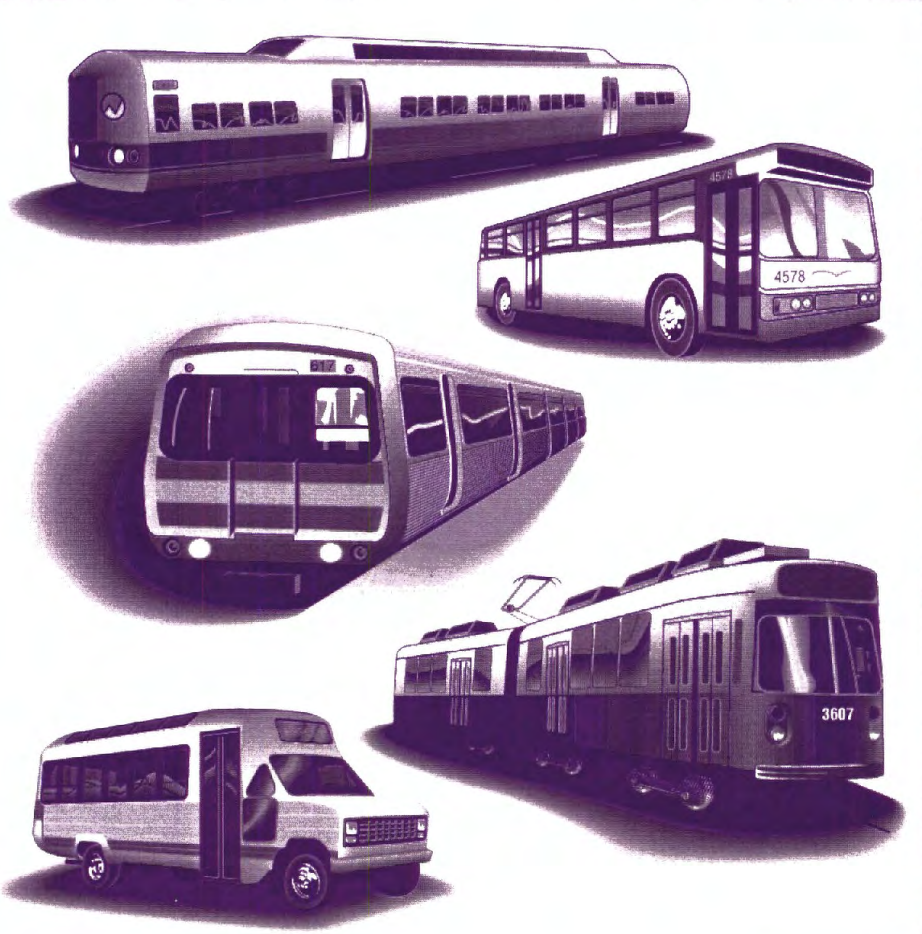
FTA-MA-90-7001-94-1
DOT-VNTSC-FTA-94-1

U.S. Department
of Transportation
**Federal Transit
Administration**

Transit System Security Program Planning Guide

U.S. Department of Transportation
Research and Special Programs Administration
John A. Volpe National Transportation Systems Center
Cambridge, Massachusetts 02142-1093

December 1994
Final Report
Reprint
November 1997



FEDERAL TRANSIT ADMINIDSTRATION

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	January 1994 Reprint November 1997	Final Report - January 1994

4. TITLE AND SUBTITLE
TRANSIT SYSTEM SECURITY PROGRAM PLANNING GUIDE

5. FUNDING NUMBERS
DTRS-57-89-D-00091
TT415/U4020

6. AUTHOR(S)
John N. Balog, Anne N. Schwarz, Bernard C. Doyle

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
KETRON Division of
The Bionetics Corporation*
350 Technology Drive
Malvern, PA 19355

KETRON Division of
The Bionetics Corporation
58 Charles Street
Cambridge, MA 02141

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-FTA-94-1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of Technical Assistance and Safety
Federal Transit Administration
U.S. Department of Transportation
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
FTA-MA-90-7001-94-1

11. SUPPLEMENTARY NOTES
*Under Contract to: U.S. Department of Transportation
Research and Special Programs Administration
Volpe National Transportation Systems Center
Cambridge, MA 02142-1093

12a. DISTRIBUTION/AVAILABILITY STATEMENT

This document is available to the public through the National Technical Information Service, Springfield, VA 22161

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The Federal Transit Administration's Safety and Security Program goal is to achieve the highest practical level of safety and security in all modes of transit. In order to protect passengers, employees, revenue, and property, all transit systems are encouraged to develop, implement, and maintain a System Security Plan and Program. Increased security should be accomplished through the use of a systems approach with both proactive and law enforcement activities clearly outlined in the Security Program Plan. The System Security Program Plan should be a complete, well thought out guide to establishing and maintaining a comprehensive Security Program for the transit system and the entire system for which it is responsible: this includes people, property, procedures, and environment. This Guide is designed to help transit systems outline and author the sections of a plan in order to implement an effective Security Program.

The Guide discusses each aspect of a security plan to ensure that when complete, the plan document will demonstrate management's commitment and policy regarding security; introduce the concept of a System Security Program; describe the transit system; establish the management of the plan; detail the Security Program by assigning responsibilities; explain how threats and vulnerabilities will be identified, assessed, and resolved; describe how the plan itself will be implemented to establish or revise the program; and describe how the Security Plan will be evaluated and modified. Additional information in the appendixes will make the complete Security Plan a valuable security reference. The Guide includes a transit security bibliography of approximately 200 documents.

14. SUBJECT TERMS
Transit, System, Security, Program, Plan, Safety, Law Enforcement, Proactive, Policy, Management, Threat, Vulnerability, Crime, Transportation, Bus, Rail, Paratransit, Employee, Procedures, Passenger, Trespass, Vandalism, Police, Guards

15. NUMBER OF PAGES
130

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Acknowledgements

The Ketron Division of The Bionetics Corporation would like to extend its full appreciation to the Federal Transit Administration, the Volpe National Transportation Systems Center, and the following individuals who were instrumental in initiating this project and bringing it to its successful conclusion:

Franz Gimmler
Deputy Associate Administrator for Safety
Federal Transit Administration

Judy Meade
Program Manager
Federal Transit Administration

Adelbert Lavery
Chief, Safety & Security Division
Volpe National Transportation Systems Center

William Hathaway
Senior Project Engineer
Volpe National Transportation Systems Center

Larrine Watson
Project Manager
Volpe National Transportation Systems Center

Debra J. Haas
Administrative Assistant
KETRON Division of The Bionetics Corporation

Jennifer E. Rimmer
Transit/Paratransit Specialist
KETRON Division of The Bionetics Corporation

Mark M. Hood
Transit/Paratransit Specialist
KETRON Division of The Bionetics Corporation

R. Benjamin Gribbon
Transit/Paratransit Specialist
KETRON Division of The Bionetics Corporation

David Chia
Transortation Planner
KETRON Division of The Bionetics Corporation

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXIMATE)

1 inch (in) = 2.5 centimeters (cm)
1 foot (ft) = 30 centimeters (cm)
1 yard (yd) = 0.9 meter (m)
1 mile (mi) = 1.6 kilometers (km)

AREA (APPROXIMATE)

1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m^2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)
1 acre = 0.4 hectare (ha) = 4,000 square meters (m^2)

MASS - WEIGHT (APPROXIMATE)

1 ounce (oz) = 28 grams (gm)
1 pound (lb) = .45 kilogram (kg)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)

VOLUME (APPROXIMATE)

1 teaspoon (tsp) = 5 milliliters (ml)
1 tablespoon (tbsp) = 15 milliliters (ml)
1 fluid ounce (fl oz) = 30 milliliters (ml)
1 cup (c) = 0.24 liter (l)
1 pint (pt) = 0.47 liter (l)
1 quart (qt) = 0.96 liter (l)
1 gallon (gal) = 3.8 liters (l)
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)

TEMPERATURE (EXACT)

$°C=5/9(°F - 32)$

METRIC TO ENGLISH

LENGTH (APPROXIMATE)

1 millimeter (mm) = 0.04 inch (in)
1 centimeter (cm) = 0.4 inch (in)
1 meter (m) = 3.3 feet (ft)
1 meter (m) = 1.1 yards (yd)
1 kilometer (km) = 0.6 mile (mi)

AREA (APPROXIMATE)

1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square meter (m^2) = 1.2 square yards (sq yd, yd^2)
1 square kilometer (km^2) = 0.4 square mile (sq mi, mi^2)
10,000 square meters (m^2) = 1 hectare (ha) = 2.5 acres

MASS - WEIGHT (APPROXIMATE)

1 gram (gm) = 0.036 ounce (oz)
1 kilogram (kg) = 2.2 pounds (lb)
1 tonne (t) = 1,000 kilograms (kg) = 1.1 short tons

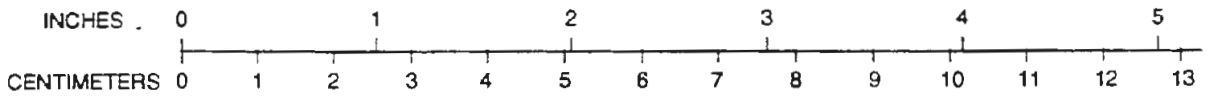
VOLUME (APPROXIMATE)

1 milliliter (ml) = 0.03 fluid ounce (fl oz)
1 liter (l) = 2.1 pints (pt)
1 liter (l) = 1.06 quarts (qt)
1 liter (l) = 0.26 gallon (gal)
1 cubic meter (m^3) = 36 cubic feet (cu ft, ft^3)
1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)

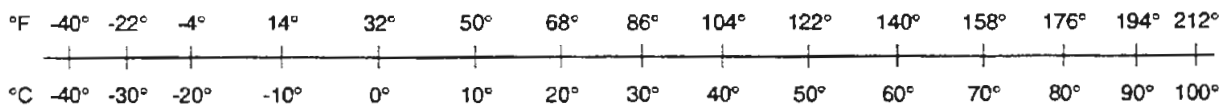
TEMPERATURE (EXACT)

$°F=9/5(°C) + 32$

QUICK INCH-CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT-CELSIUS TEMPERATURE CONVERSION



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50. SD Catalog No. C13 10286.

Updated 8/1/96

Contents

Appendixes

Introducing This Guide

What this Section Contains:

- **Role of the Federal Transit Administration (FTA)**
- **About This Guide**
- **Five Steps to a Successful Security Program Plan**
- **Outline of Transit System Security ProgramPlan**
- **Your Checklist**
- **Bibliography (that will help you prepare your Plan)**
- **Definitions (that may be useful)**

Role of the FTA

The goal of the Federal Transit Administration's (FTA's) Safety and Security Program is to achieve the highest practical level of safety and security in all modes of transit. To this end, the FTA has continuously promoted the awareness of transit safety and security throughout the transit community by establishing programs to collect and disseminate information on safety/security concepts, practices, and guidelines that transit systems can apply in the design of their procedures and by which to compare local actions.

The FTA encourages all transit systems, sometimes referred to as "authorities" or "properties", to develop and implement a Transit System Security Plan and Program which covers passengers, vehicles, and facilities. The FTA also recognizes that every transit system has a variety of intensive demands for its resources.

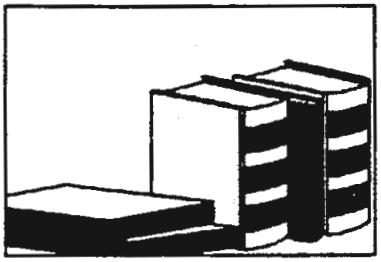
The FTA and assisting organizations prepared this Guide in order to assist transit properties in developing their Security Plan and Program. This Guide has been designed to help the transit system outline and write the various sections of a Security Plan (Plan) in order to implement an effective Security Program (Program). Each section of the actual plan to be produced by the system is fully discussed in this Guide. It is believed that by using this Guide, the person or department responsible for transit security can quickly, efficiently, and effectively develop an appropriate Plan.

The Guide has been designed so that you can read a chapter and then prepare the comparable section in your Plan. For example, Chapter 1 explains the "Opening Pages to the System Security Plan"; Chapter 2 explains Section I that would be the "Introduction to Security System," etc. In some cases, information already produced by the system may be easily inserted after slight editing. In other situations, very specific text can be used with minimal editing. The Guide also offers examples to stimulate you in the development of creative applications.

Five Steps to a Successful Security Program Plan

Step 1

Read the Guide thoroughly before starting the Plan development process.

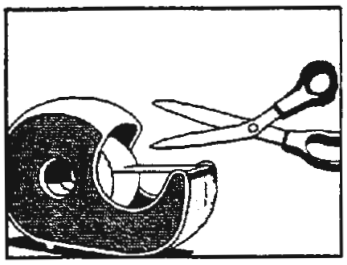


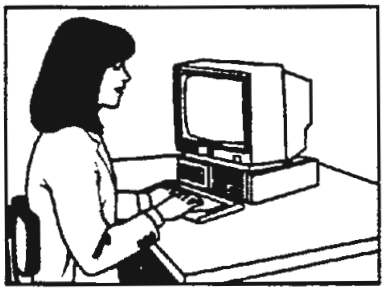
Step 2

Collect all of the relevant materials from existing files.

Step 3

Modify the outline to reflect the system size and the operation.





Step 4

Use the examples in this Guide, such as sample memos, etc.

Step 5

Congratulate yourself on a job well done!

Outline of Transit System Security Program Plan

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

Outline of Transit System Security Program Plan (Concluded)

IV System Security Program: Roles and Responsibilities
- 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
  1. Security Testing and Inspections
  2. Data Collection
  3. Reports
  4. Security Information Flow
- B. Threat and Vulnerability Assessment
  1. Responsibility
  2. Data Analysis
  3. Frequency and Severity
- C. Threat and Vulnerability Resolution
  1. Emergency Response
  2. Breach Investigation
  3. Research and Improvements
  4. Eliminate, Mitigate, or Accept

VI Implementation and Evaluation of System Security Program Plan
- A. Implementation Goals and Objectives
- B. Implementation Schedule
- C. Evaluation
  1. Internal Review — Management
  2. 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 Appendixes

Your Checklist

When your Plan is concluded, it should be a complete, well-thought-out guide to establishing and maintaining a comprehensive Program for your transit system and all elements for which it is responsible. This includes people, property, procedures, and the environment. Increased security should be accomplished through the use of a systems approach, with both proactive and law enforcement activities clearly outlined in the Program Plan. Your completed Plan should have

- ☑ demonstrated management's committment and policy regarding security,
- ☑ introduced the concept of a Program,
- ☑ described the transit system,
- ☑ established the management of the Plan,
- ☑ detailed the Program by assigning responsibilities,
- ☑ explained how threats and vulnerabilitieswill be identified, assessed, and resolved,
- ☑ described how the Plan itself will be implemented to establish or revise the Program, and
- ☑ describe how the Plan will be evaluated and modified

Additional information in the appendixes will make this a complete Plan and a valuable security reference.

One Final Note...

Remember, the goal of your Plan is to implement a Program which maximizes System Securityvia a set of system-specific objectives. Information on the intent of your Program should include who is involved, their functions, and how they relate to the stated goals and objectives. Careful consideration must be given this relationship.

Bibliography

The following is a bibliography of suggested readings that will help you to prepare your Plan.

Abkowitz, M. *Role of Microcomputers in the Transportation Environment.* Roades and Transportation Association of Canada, September 1984.

Already a Blot on the Blue Line. Los Angeles Times, p. B8, November 4, 1989.

An Analytical Safety and Security Program for Public Transportation in Southeast Michigan. Southern Michigan Council of Governments. Report No. UMTA-MI-06-0038-85-1, June 1984.

Andel, Henk van. *Crime Prevention that Works: The Care of Public Transport in The Netherlands.* The British Journal of Criminology, Vol. 29, pp. 47-56, Winter 1989.

Andrle, S.J., Barker, B., Golenberg, M., and Richards, L.G. *Security Considerations in the Design and Operation of Rapid Transit Stations (Abridgment).* Transportation Research Record, N760, pp. 42-45, 1980.

An Organized Approach to Crowd Control. Athletic Purchasing & Facilities, May 1983.

Are the Animals Running the Farms? Security Management, Vol. 25, No. 1, pp. 41-44, January 1981.

Assaults on Bus Staff and Measures to Prevent Such Assaults: Report on The Working Group on Violence to Road Passenger Transport Staff Under the Chairmanship of HMSO London. 1986.

Assessing the Social Environment. U.S. Department of Housing and Urban Development, Office of Policy Development and Research, Washington, DC, U.S. Government Printing Office, 1980.

Atkins, Steven T. *Critical Paths: Designing for Secure Travel.* 1989.

Austin, T.L. and Buzawa, E.S. *Citizen Perceptions on Mass Transit Crime and Its Deterrence: A Case Study.* Transportation Quarterly, Vol. 38, No. 1, pp. 103-120, January 1984.

Ayre, F. *Lighting for an Integrated Public Transport System.* Light J (Rugby Engl), Vol. 51, No. 4, pp. 233-235, 1986.

Balog, J.N., Chia, D., Schwarz, A.N., and Gribbon, R.B. *Accessibility Handbook for Transit Facilities.* U.S. Department of Transportation, July 1992, Reprint January 1993.

Balog, J.N., Gribbon, R.B., Watson, L., Hathaway, W., Schwarz, A.N., and Doyle, B.C. *Guidelines for the Development of Passenger, Vehicle, and Facility System Security Program Plans.* Transportation Research Board, Paper #930651, January 1993.

Balog, J.N. *Safety Planning Information Directed to Emergency Response: Presentation Guide.* S.P.I.D.E.R. Program: West Virginia Department of Transportation, Charleston, WV, November 29, 1989.

Balog, J.N. *Safety Planning Information Directed to Emergency Response: Resource Manual Guide.* S.P.I.D.E.R. Program: West Virginia Department of Transportation, Charleston, WV, November 29, 1989.

Balog, J.N. *Training Module: Recommended Procedures for Increased Security Awareness.* October 31, 1991.

Balog, J.N., Ketola, H.N., Varker, F.A., McInerney, T.T., and Scott, R.E. *Evacuation and Rescue of Elderly and Disabled Passengers from Paratransit Vans and Buses.* U.S. Department of Transportation, Urban Mass Transportation Administration, Transportation Systems Center, February 1985.

Barrier Technology Handbook. Nuclear Security Systems, Albuquerque, New Mexico, 1979.

Batiste, F. *Invasion of the Vandals.* Mass Transit, Vol. 20, No. 3, pp. 50-5, March 1991.

Beller, A., Garelik, S., and Cooper, S. *Sex Crimes in the Subway.* Criminology, Vol. 18, No. 1, pp. 35-52, May 1980.

Berry, C.R. and Stuart, D.G. *Electromechanical Transit Security Equipment.* Report No. UMTA-79-185, UMTA-IT-06-0247-83-1, Cambridge, MA, 1982.

Bloom, Richard F. *Close Circuit Television in Transit Stations: Application Guidelines.* Dunlap & Associates, Inc., Report No. ED-80-1, DOT-TSC-UMTA-80-33; UMTA-MA-06-0048-80-5, Cambridge, MA, August 1980.

Bloomberg, II and Ahmed, S. *Underground Railroad Police Communications System Interface With Above Ground Public Safety Communications System.* Joint Asmeieee Railroad Conference, pp. 147-156, New York, 1988.

Bowles, Anne L. *Schools Trying Video to Keep Riders Quiet.* The Philadelphia Inquirer, September 13, 1992, P. B1.

Bowman, M.A. *Uniform Transit Safety Records System for the Commonwealth of Virginia.* Report No. VHTRC-81-R39, DOT-I-82-21, Charlottesville, 1981.

Budd, Jeff. *Graffiti: Vandalism Masquerades as Art.* Transit Policing, Vol. 1, No. 1, pp. 12-13, Fall 1991.

Burstein, Harvey. *Industrial Security Management.* New York, Praeger, 1977.

Bus Transportation: National and General Studies. Report No. PB83 -808147, Springfield, VA, 1983.

Butcher, Clive. *Underground Communications Keep Passengers Safe and Informed.* Railway Gazette International, Vol. 146, No. 10, pp. 787, 789-790, October 1990.

Bynum, Timothy S. and Purri, Dan M. *Crime and Architectural Style: An Examination of the Environmental Design Hypothesis.* Criminal Justice and Behavior, Vol. 11, pp. 179-196, June 1984.

Caso, Peter J. *Panhandling & The Law in the New York City Subway,* Transit Policing, Vol. 1, No. 1, Fall 1991, p. 17.

Chelimsky, E. *Security and the Small Business Retailer.* U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Program Models, Washington, DC, U.S. Government Printing Office, February 1979.

Chess Match with Thieves, and Tokens are the Pieces. The New York Times, p. A15, May 30, 1990.

Connell, W.M. *Safety Priorities in Rail Rapid Transit, Volume 1 — Report.* Washington, DC, 1974.

Content Guidelines for Bus System Safety Program Plans — Draft. American Public Transit Association Safety and System Assurance Liaison Board.

Controlling the Rock Concert Crowd, Security World, June 1980.

Cooney, N.A. *Development of an Automated Security Incident Reporting System (SIRS) for Bus Transit.* Report No. DOT-TSC-UMTA-86-13, 1986.

Cosby, S. *A Method for Measuring the Revenue Loss Due to Fraud Within a Public Transport Undertaking.* Traffic Engineering & Control, Vol. 26, No. 2, pp. 59-61, February 1985.

Crime and Security Measures on Public Transportation Systems: A National Assessment. Southeast Michigan Council of Governments, July 1981.

Crime in Mass Transit. Hearing Before a Subcommittee of the Committee on Appropriations, United States Senate, 101st Congress, 2nd Session, September 17, 1990. Special Hearing. Washington, DC, 1991.

Crime Prevention: Protecting PHAs. Journal of Housing, Vol 43, p. 165, July/August 1986.

Crowe, Timothy. *Crime Prevention Through Environmental Design: Application of Architectural Design and Space Management Concepts.* Stoneham, MA, Butterworth-Heinman, 1991.

Daetz, D. and Bebendorf, M. *A Socioeconomic Impact Assessment of the Los Angeles Automatic Vehicle Monitoring (AVM) Demonstration.* SYSTAN, Inc., Report No. UMTA-MA-06-0126-82-2, DOT-TSC-UMTA-82-42, October 1982.

Delaware Administration for Regional Transit (DART) Fare Handling and Operator Performance Analysis. Burns International Security Services, Report No. DE-09-0006, July 1983.

Delinquency and Vandalism in Public Transport. Report of the 77th Round Table on Transport Economics, Paris, October 1987.

Demetsky, Michael J. *Station Design Methodology.* Conference: Proceedings of a National Conference on the Planning and Development of Public Transportation Terminals, Silver Spring, MD, September 1980.

Department of Transportation Physical Security Manual. U.S. Department of Transportation, Washington, DC, DOT, 1977.

Derr, K.E. and Ferreri, M.G. *Field Testing of Electronic Registering Fareboxes.* Booz-Allen and Hamilton, Bethesda, MD, Report No. UMTA-MA-06-0120-86-2, DOT-TSC-UMTA-86-9, February 1987.

Deschamps, Scott. *The BC Transit Fare Evasion Audit: A Description of Situational Crime Prevention Process.* Security Journal, Vol. 2, No. 3, 1991.

Deschamps, Scott. *Vancouver Regional Transit System: Environment and Design Challenge BC Transit Police.* Transit Policing, Vol. 1, No. 1, pp. 13-14, 19, Fall 1991.

Diamond, Norman. *Is That Pass Authentic? A New & Innovative Solution to the Many Problems of Transit Pass Counterfeiting.* Conference Presentation, General Farebox Incorporated.

Domestic Terrorism. Prevention Efforts in Selected Federal Courts and Mass Transit Systems. General Accounting Office, Report No. GAO/PEMD-88-22, June 1988.

Dorer, R.M. and Hathaway, W.T. *Safety of High Speed Magnetic Levitation Transportation Systems.* Report No. DOT-VNTSC-FRA-90-3, Cambridge, MA, 1991.

DOT Announces Interagency Grants for Homeless Living in Transit Facilities. USDOT News, September 6, 1991.

Driver Training Program for Small Urban and Rural Transit Vehicle Operators. Ohio Department of Transportation.

Dugger, Celia W. *Threat Only When on Crack, Homeless Man Foils System.* The New York Times, September 3, 1992.

The Emerging Subway Thief: Frustrated, Angry and Impatient. The New York Times, p. A13, June 25, 1990.

Englisher, L.S. *Late-Night Shared-Ride Taxi Transit in Ann Arbor, Michigan.* Report No. UMTA-MA-06-0049-84-7, DOT-TSC-UMTA-84-28, October 1984.

Falanga, M. *Reducing Crime Through Design in the Chicago Subway System.* Ann Arbor, MI, 1989.

Fare Beaters in Subway Pay in the End, In Sweat. The New York Times, p.10, February 18, 1991.

Fare Beating Rising Again Despite Curbs. New York Times, p.A1, August 16, 1991.

Fear in the Subway: Riders Adopt Tactics to Ward Off Danger. The New York Times, p.1, September 9, 1990.

Fruin, J.J., Guha, D.K., and Marshall, R.F. *Pedestrian Falling Accidents in Transit Terminals.* Report No. DOT-TSC-UMTA-84-36, 1990.

Gaylord, M.S. and Galliher, J.F. *Riding the Underground Dragon: Crime Control and Public Order on Hong Kong's Mass Transit Railway.* The British Journal of Criminology, Vol 31, pp. 15-26, Winter 1991.

Gardiner, R.A. *Design for Safe Neighborhoods: the Environmental Security Planning and Design Process.* U.S. Department of Justice, Law Enforcement Assistance Administration, National Institute of Law Enforcement and Criminal Justice, Washington, DC, U.S. Government Printing Office, September 1978.

Goldsack, P.J. *Video Cameras Cut U.K. Bus Assault Statistics.* Mass Transit, Vol. 14, No. 6, pp. 13-14, June 1987.

Grand Central Terminal will be Bathed in Light. The New York Times, p. A17, November 19, 1989.

Greenburg, M.A. *The ABCs of Subway Safety.* Campus Law Enforcement Journal, Vol. 15, No. 4, pp. 8-11, Castleton State College, August 1985.

Guidelines for Planning, Design and Operation of Rail Commuter Parking Facilities. Chicago, IL, 1990.

Gunn, D.L. *The Human Story Behind The Graffiti.* Railway Gazette International, Vol. 141, pp. 35-37+, January 1985.

Handbook. Guide for Developing a Transit Safety and Security Information System. Southeast Michigan Council of Governments, 1986.

Hargadine, E.O. *Case Studies of Transit Security on Bus Systems.* Report No. UMTA-VA-06-0088-83-1, McLean, VA, 1984.

Hargadine, E.O. and Scott, G. *Documentation and Assessment of Transit Security Data Reporting and its Utilization.* Mandex, Vienna, VA, March 1985.

Hathaway, W.T. *System Security in Mass Transit.* American Defense Preparedness Association Joint Government-Industry Symposium, Cambridge, MA, 1988.

Hathaway, W.T., and Doyle, B. Jr. *A Proposed Methodology for Addressing Terrorism in Transportation.* Fourth Annual Joint Government-Industry Symposium, Arlington, VA, 1988.

Hathaway, W.T., Heimann, D.I., and Hammar, P.K. *Development of a Graphics Based Automated Emergency Response System (AERS) for Rail Transit Systems.* Report No. DOT-TSC-UMTA-89-1, 1989.

Hathaway, W.T. and Markos, S.H. *Recommended Emergency Preparedness Guidelines for Urban, Rural, and Specialized Transit Systems.* Report No. DOT-VNTSC-UMTA-91-1, 1991.

Hathaway, W.T., Markos, S.H., and Balog, J.N. *Recommended Emergency Preparedness Guidelines for Elderly and Disabled Rail Transit Passengers.* Report No. DOT-TSC-UMTA-89-4, 1991.

Hathaway, W.T., Markos, S.H., and Pawlak, R.J. *Recommended Emergency Preparedness Guidelines for Rail Transit Systems.* Rpt. No. DOT-TSC-UMTA-84-26, 1985.

Hemphill, Charles F. *Management's Role in Loss and Prevention.* New York, Amacon, 1976.

Hoel, L.A. *Guidelines for Planning Public Transportation Terminals.* Transportation Research Record, N817, pp. 36–41, 1981.

Hoffmann, P.S. *Market East Station. What Makes it Unique.* Focus/Philadelphia Business Newsweekly, January 1985.

Homeless and bus terminals. The Times-Picayune, New Orleans, September 2, 1992.

Hong Kong's MTR Opens Island Line. China Transport, Vol. 1, No. 1, China Transport Publications Limited, 1985.

Improving Public Transportation to Non-CBD Industrial Centers. Steinway, Queens, Hunts Point, The Bronx, and Greenpoint/Williamsburg, Brooklyn. Report No. UMTA-NY-09-0054-86-1, New York City 1986.

Innovation in Public Transportation. UMTA, Report No. UMTA-MA-06-0086-85-1, DOT-TSC-UMTA-85-2, Washington, DC, December 1984.

Instructor's Manual for Emergency and Accident Handling Procedures (Mass TransitInstructor Orientation and Training Course). USDOT, Transportation Safety Institute.

Instructor's Manual for Passenger Relations (Mass Transit Instructor Orientation and Training Course). USDOT, Transportation Safety Institute.

Jacobs, Bernard M. *Subway Security.* Mass Transit, July/August 1992, p. 45.

Jacobson, I., Richards, L., Leiner, C.T., Hoel, L., and Braden, A. *Automated Guideway Transit System Passenger Security Guidebook (Final Report).* Report No. DOT-TSC-UMTA-80-1, UMTA-MA-06-0048-79-7, Cambridge, MA, March 1980.

Jeffrey, C. Ray. *Crime Prevention Through Environmental Design.* Beverly Hills, CA, Sage, 1977.

Jones, R.E. *Counterfeit Pass Prevention.* Metro, Vol. 82, No. 2, March 1986.

Kabundi, M. and Normandeau, A. *Crime in the Montreal Subway.* International Criminal Police Review, Vol, 42, No. 406, pp. 24-27, May 1987.

Jones, C.J. *Transit Fare Revenue Accountability and Protection Guidelines.* Report No. UMTA-DC-0521-89-1, Washington, DC, 1989.

Kelling, George L. and Bratton, William J. *Transit Police and Their Communities.* Transit Policing, Vol. 1, No. 1, pp. 1, 5-6, 18, Fall 1991.

Kennedy, Daniel B. *Inadequate Security and Premises Liability: How Criminals Think.* Trail, Vol. 27, pp. 56-60, June 1991.

Keeney, K. *A New Home for the Homeless.* Modern Railroads, Vol. 45, No. 9, pp. 38-41, May 1990.

Kenney, D.J. *Crime on the Subways: Measuring the Effectiveness of the Guardian Angels.* Justice Quarterly, Vol. 3, No. 4, pp. 481-496, December 1986.

Kenney, D.J. *Crime, Fear, and the New York City Subways: The Role of Citizen Action.* ISBN No. 0275923223, New York, 1987.

Kenton, Edith. *Bus Transportation: National and General Studies.* Springfield, VA, 1980.

Kiersh, E. *Protecting the Commuter.* Police Magazine, Vol. 3, No. 5, pp. 36-43, September 1980.

Krahn, Harvey and Kennedy, Leslie W. *Producing Personal Safety: The Effects of Crime Rates, Police Force Size, and Fear of Crime.* Criminology, Vol 23, p. 710, November 1985.

Krupat, Edward and Kubzansky, Philip E. *Designing to Deter Crime.* Psychology Today, Vol. 21, pp. 58-61, October 1987.

Kuner, R. *Transit Crime Programs.* Proceedings, Metropolitan Conference on Public, pp. 389-397, 1987.

Levine, N. and Wachs, M. *Factors Affecting the Incidence of Bus Crime in Los Angeles, Vol. 1 Final Report.* Report No. DOT-I-85-28, Washington, DC, January 1985.

Levine, N. and Wachs, M. *Tracking Crime on Buses.* TRNews, N127, pp. 18-22, November 1986.

Levine, N. and Wachs, M. *Bus Crime in Los Angeles: Measuring the Incidence and Public Impact.* Transportation Research, Part A: General, Vol. 20A, No. 4, pp. 273-293, July 1986.

Levine, N. and Wachs, M. *Bus Crime: The Skeleton in the Closet.* Its Review, Vol. 8, No. 3, pp. 4-5, May 1985.

Levine, N. and Wachs, M. *Factors Affecting the Incidence of Bus Crime in Los Angeles, Volume 2, Appendices.* Report No. UMTA-CA-06-0195-85-2, Los Angeles, CA, 1985.

The Link Between Crime and the Built Environment: The Current State of Knowledge. Volume 1. U.S. Department of Justice, National Institute of Justice, Washington, DC, U.S. Government Printing Office, December 1980.

The Lowest Crime in New York. Los Angeles Times, p. A1, June 4, 1991.

Lynch, G. and Atkins S. *The Influence of Personal Security Fears on Women's TravelPatterns.* Transportation, Vol. 15, No. 3, pp. 257-277, 1988.

Manegold, Catherine S. *Port Authority Helps Homeless Find an Exit.* The New York Times, August 17, 1992, p. A1.

Mangelsdorff, D. and Kohler, T. *Chicago Transit Authority Turnstile Pass Reader System. Final Report.* Report No. UMTA-IL-06-0049-87-1, Chicago, IL, August 1987.

Martin, C.A. *Security and the Mass Transit System.* Monticello, IL, 1981.

Massachusetts Legislative Research Council — Report Relative to Crime on Public Transportation Systems. Report No., House No. 5955, Boston, MA, 1980.

McCormick, Grant. *Close Circuit Television for Vancouver's Skytrain.* WESCANEX '86 Conference Record, Vancouver, BC, Can, 1986.

McDonald, M. *Transportation Research Group, Department of Civil Engineering, University of Southamptom: Research Report 1987.* Printerhall Limited, Traffic Engineering and Control, Vol. 29, No. 2, pp. 84-90, February 1988.

Mellor, A. *The Missing Millions: A Study of the Losses Due to Vandalism and Fraud.* Planning and Transport Research Computation, pp. 53-66, 1988.

Moore, Harley L. III, Scott, Wade A., and Lindell, Harry. *Downtown People Mover System Security: Detroit and Miami Responses.* Conference: Automated People Movers: Engineering and Management in Major Activity Centers, Miami, FL, March 1985.

Moving America: New Directions, New Opportunities. A Statement of National Transportation Policy. Strategies for Action. Department of Transportation Office of the Secretary, Washington, DC, February 1990.

Murphy, Joan H. *Providing a Safe Haven.* Security Management, Vol. 33, pp. 38-45, April 1989.

National Conference on Mass Transit Crime and Vandalism, Compendium of Proceedings held in New York City on October 20-24, 1980. Report No. UMTA-NY-06-0083, Albany, NY, 1981.

Newman, D.A. *Integrating Bicycles and Transit in Santa Barbara, California.* Los Altos, California, Rpt No. UMTA-MA-06—114-83-1, DOT-TSC-UMTA-83-10, March 1983.

New York City Transit Authority. *Access Improvements to the Staten Island Rapid Transit System. Final Report.* Report No. UMTA-NY-08-0102-86-1, New York City, 1986.

Night-Vision Goggles Help Transit Police. Metro Magazine, July/August 1992, p. 11.

O'Block, R.L. and Donnemeyer J.F. *Security and Crime Prevention.* 2nd ed. Boston, Butterworth-Heinemann, 1991.

O'Mahoney, Timothy. *Keeping Watch Over Mass Transit.* Security Management, Vol. 34, pp. 50-54, January 1990.

Oxley, P.R. *Assaults on Bus Staff in Great Britain.* Transportation Research Record, N1108, pp. 27-30, 1987.

Passenger Safety in Metropolitan Railways. International Union of Public Transport, UITP Revue, Vol. 35, No. 1/86, pp. 14-20, 1986.

Patrol Strategies Catalog. New York City Transit Police Department, 1992.

Patterson, A. H. and Ralston, P.A. *Fear of Crime and Fear of Public Transportation Among the Elderly, (Final Report April 1983).* Report No. UMTA-PA-11-0026-84-1, Pennsylvania, 1983.

Paumier, Jean-Michel. *Paris Metro Counters Crime.* Railway Gazette International, Vol. 146, No. 10, pp. 781-782, October 1990.

Pawlak, Robert J., Snow, Robert M., and Metcalf, Marion E. *Annotated Bibliography of Rail*

Transit Safety 1975—1980, with Emphasis on Safety Research and Development (Final Report 1975—80). Report No. DOT-TSC-UMTA-MA-06-0098, Cambridge, MA, 1981.

Pearlstein, A. and Wachs, M. *Crime in Public Transit Systems: An Environmental Design Perspective.* Transportation (Netherlands), Vol. 11, No. 3, pp. 277-297, September 1982.

Petrie, J.F. and Hathaway, W.T. *Development of an Automated Emergency Response System (AERS) for Rail Transit Systems.* Report No. DOT-TSC-UMTA-84-27, 1985.

Petty Thefts Disable New York Turnstiles a Few Tokens at a Time. The New York Times, p. A16, August 8, 1989.

Planning for Housing. U.S. Department of Housing and Urban Development, Office of Policy Development and Research, Washington, DC, U.S. Government Printing Office, 1979.

Preliminary Safety Investigation of the New York Metropolitan Transportation Authority. USDOT, Washington, DC, 1991.

Problems of Business and Industrial Security. New York, NY, Practicing Law Institute, 1971.

Prowe, G.J. *Transit Security: A Description of Problems and Countermeasures.* Report No. DOT-TSC-UMTA-84-22, 1986.

Quidgley, C.M. *Comparative Study of Four Transit System Police Departments.* Massachusetts Committee on Criminal Justice, 1981.

Ray, C., Stuart, D., Thomson, D., Rouse, V., and Botts, J. *Predicting Automated Guideway Transit System Station Security Requirements.* Report No. DOT-TSC-UMTA-80-5, Cambridge, MA, March 1980.

Reis, A.P. *Black Commuting in Pretoria: Attitudes Towards Crime Levels.* South Africa, Report No. NITRR BCP 10, November 1982.

Reiss, A.J. *Policing a City's Central District: The Oakland Story.* U.S. Department of Justice, Washington, DC, U.S. Government Printing Office, March 1985.

Reiss, S., Sandler, R., and Schoenbrod, D. *Subway Scofflaws: A Proposal to Improve Enforcement.* New York Affairs, Vol. 8, No. 3, New York University, 1984.

Richards, Larry G., Jacobson, Ira D., and Hoel, Lester A. *Passenger Security in Public Transportation: Psychological and Environmental Factors.* Conference: Human Factors in Transport Research, Swansea, Wales, September 1980.

Reports of the Latest Crimes Frighten Subway Passengers. The New York Times, p. A19, June 15, 1989.

Richards, L.G. and Hoel, L.A. *Planning Procedures for Improving Transit Station Security.* Report No. UVA/529036/CE80/106, DOT/RSPA/DPB-50-80/14, Virginia University, February 1980.

Richards, L.G. and Hoel, L.A. *Planning Procedures for Transit Station Security.* Virginia University, Traffic Quarterly, Vol. 34, No. 3, pp. 355-375, July 1980.

Richards, L.G. and Jacobson, I.D. *Passenger Value Structure Model. Annotated Guideway Transit Technology Program.* Report No. DOT-TSC-UMTA-80-23, UMTA-MA-06-0048-79-8, Darien, CT, 1980.

Riley, N.E. and Dean, D.L. *Crime and Security at Intercity Bus Stations.* Report No. DMT-130, Sacramento, CA, October 1984.

Riley, N.E. and Dean, D.L. *Bus Station Security: Crime at Intercity Bus Locations.* Transportation Research Record N1012, pp. 56-64, 1985.

Rodano, E.M. *Technical Assistance and Safety Programs: Fiscal Year 1988 Project Directory.* Report No. UMTA-UTS-22-89-1, January 1989.

Roland, H.E. and Moriarity B. *System Safety Engineering and Management.* New York, NY, John Wiley & Sons, Inc., 1990.

Safety Information Reporting and Analysis System (SIRAS) Instruction Manual For Heavy Rapid Rail Transit (RRT) Reporting Forms. Report No. UMTA-MA-06-0152-86-1, DOT-TSC-UMTA-86-5, 1986.

Safety on The Metro. Railway Gazette International, Vol. 145, No. 1, pp. 23-41, January 1989.

Sanso, B., Mahseredjian, J., and Mukhedkar, D. *Total Accident Probability of a Metro System.* Chicago, 1984.

Scheer, T. *Goal of Transit Police is Making Commute Safe.* Metro, Vol. 85, No. 7, November 1989.

Schwartz, R. *The Homeless: The Impact on The Transportation Industry, Volume I.* The Port Authority of New York and New Jersey, 1988.

Schwartz, R. *The Homeless: The Impact on The Transportation Industry, Volume II, Appendices.* The Port Authority of New York and New Jersey, 1988.

Schwartz, R. *The End of the Line: The Homeless and The Transportation Industry.* Portfolio, pp. 38-46, 1991.

Security Update Shows Successes. Reed Business Publishing Limited, City Transport, Vol. 2, No. 4, p. 34, December 1987.

Self-Service Fare Collection State-Of-The-Art. Organization for Environmental Growth, Washington, DC, August 1983.

SEPTA Held Not Liable for Assault on Passenger. Mass Transit Lawyer/Administrator, Vol. 3, No. 15, August 19, 1992.

Strauchs, J.J. *Urban Mass Transit Security.* American Society for Industrial Security Standing Committee on Transportation Security, Vol. 26, No. 2, February 1982.

Sturman, A. *Damage on Buses — The Effects of Supervision.* Designing Out Crime, p. 31-38, 1980.

Subway Crime Drops Sharply at Year's End. But for 1990 Overall, Felonies Rose 8.4%. The New York Times, p. B3, February 15, 1991.

Subway Felonies Down by 13%. Overtime Police Patrols Praised. The New York Times, p. B14, November 15, 1991.

Sullivan, J.P. *Managing Homelessness in Transportation Facilities.* New England Journal of Human Services, Vol. 6, No. 2, pp. 16-19, 1986.

Survey into Women's Transport Needs: Summary Commenting on the Results of the Survey into Women's Transport Needs. Greater London Council Transport Committee, London, England, May 1985.

Sussman, E. Donald and Richards, Larry G. *Transit Station Security.* Conference: Proceedings of a National Conference on the Planning and Development of Public Transportation Terminals, Silver Springs, MD, September 1980.

Swain, D. *Crime on the London Underground.* Planning and Transport Research and Computation, pp. 239-246, 1988.

Symes, D.J. *Automatic Vehicle Monitoring — Past, Present and Future.* New Jersey Report No. IEEE-80-CH1601-4, HS-030 446, 1980.

System Safety Glossary for Transit. USDOT, Transportation Systems Center, Cambridge, MA, 1988.

Taking Back the Subway for the People of New York. The New York City Transit Police Vision for the 1990s.

Thieves Annually Steal Millions in Equipment From Transit Agency. The New York Times, P. A19, May 3, 1990.

Thompson, R.E. *Use of Radios in Rail Transit Operations, Volume 1. Review of Existing Practices.* Report No. UMTA-IT-06-0190-89-2, May 1989.

Thompson, R.E. and Kangas, R. *Use of Radios in Rail Transit Operations. Volume 2. Transit Authorities' Responses.* Rpt No. UMTA-IT-06-0190-89-3, November 1989.

Tidbury, G.H. *Getting Rollover Strength.* Transport Engineer, pp. 20-21, 1982.

Transit Security Guidelines Manual. American Public Transit Association, Washington, DC, Feburary 1979.

Transit System Security. Metro, Bobit Publishing Company, November 1985.

Transit Turns to Hi Tech. Progressive Railroading, Vol. 28, No. 8, Murphy -Richter Publishing Company, Chicago, IL, August 1985.

Transportation Safety Information Report. Second Quarter 1985. Transportation System Center, Cambridge, MA, Report No. DOT-TSC-RSPA-85-8, HS-039 574, October 1985.

Turnstile Justice. The New York Times, p. A14, June 19, 1990.

UMTA Technical Assistance 1985 Training Directory. UMTA, Washington, DC, 1985.

UMTRIS Searches Pertaining to Security and Safety Problems of Bus and Cab Drivers 14 Selections. National Research Council Transportation Research, pp. 4-19, June 1986.

Urban Mass Transportation Administration. *Agenda for the Urban Mass Transportation Administration's Transit Planning and Research Program.* Report No. UMTA-UT-06-0001-91-1, Washington, DC, January 1991.

VanAndel, H. *Crime Prevention That Works: The Care of Public Transport in the Netherlands.* Gravenhage, Netherlands, 1988.

Vandalism in Metropolitan Railways. International Union of Public Transport. UITP Revue, Vol. 32, No. 4, pp. 351-356, 1983.

Volpe, J.A. *Preliminary Safety Investigation of the New York Metropolitan Transportation Authority.* Cambridge, MA, 1991.

When a Bus Ride Turns to Fear. UCLA Graduate School of Architecture and Urban Planning, UCLA Architecture and Planning, pp. 26-31, 1985.

When Crime on the Underground is Good News. Australian Police Journal, Vol. 39, No.3, pp. 116-11, September 1985.

Willis, J. *Emergency Alarm Systems: Improved Emergency Alarm Response System.* Report No. UMTA/TX/06/0042-86/1, October 1986.

Willis, J., Brooks, D., Bumpers, V., Jones, R., Kelly, T., and Oliver, H. *Emergency Alarm Systems: Improved Emergency Alarm/Response System. Final Report.* Report No. UMTA-TX-06-0042-86-1, Houston, TX, January 1986.

Wong, Y.F. *Safety From Crime "Down the Tubes" in Hong Kong.* Police Journal, Vol. 58, No. 3, pp. 265-26, September 1985.

Zaza, Robert N. *Metro Transit Police: Protecting Mass Transit in Nation's Capital.* Transit Policing, Vol. 1, No. 1, pp. 10-11, Fall 1991.

Zimmerman, S. *National Transportation Data Needs for the 1990s: Transit Strategic Planning.* Transportation Research Record, N1271, pp. 20-22, 1990.

15 More Areas in Subways to be Closed. The New York Times, p. B1, March 29, 1991.

1981 Guidelines for Design of Rapid Transit Facilities. American Public Transit Association, June 1981.

Definitions

The U.S. Department of Transportation, Volpe National Transportation Systems Center has prepared a document entitled System Safety Glossary for Transit, which contains many definitions that may be useful. The following are a few of the definitions that may be used verbatim.

Emergency:	A situation which is life threatening to passengers, employees, or other interested citizens or which causes damage to any transit vehicle or facility or results in the significant theft of services and reduces the ability of the system to fulfill its mission.
Procedures:	Established and documented methods to perform a series of tasks.
Redundancy:	The existence of more than one means of accomplishing a given function.
Safety:	Freedom from danger.
Security:	Freedom from intentional danger.
Security Breach:	An unforeseen event or occurrence which endangers life or property and may result in the loss of services or system equipment.
Security Incident:	An unforeseen event or occurrence which does not necessarily result in death, injury, or significant property damage but may result in a minor loss of revenue.
Security Threat:	Any source that may result in a security breach, such as a vandal or disgruntled employee; or an activity, such as an assault, intrusion, fire, etc.
System:	A composite of people (employees, passengers, others), property (facilities and equipment), environment (physical, social, institutional), and procedures (standard operating, emergency operating, and training) which are integrated to perform a specific operational function in a specific environment.
System Security:	The application of operating, technical, and management techniques and principles to the security aspects of a system throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources.
System Security Management:	An element of management that defines the system security requirements and ensures the planning, implementation, and accomplishment of system security tasks and activities.

System Security Program: The combined tasks and activities of system security management and system security analysis that enhance operational effectiveness by satisfying the security requirements in a timely and cost-effective manner through all phases of a system life cycle.

Threat: Any real or potential condition that can cause injury or death to passengers or employees or damage to or loss of transit equipment, property, and/or facilities.

Threat Analysis: A systematic analysis of a system operation performed to identify threats and make recommendations for their elimination or mitigation during all revenue and nonrevenue operation.

Threat Index: A quantitative measure interfacing the numerical probability of a threat with the severity of the threat.

Threat Management (Loss Control): An element of the system security management function that evaluates the security effects of potential threats considering acceptance, control, or elimination of such threats with respect to the expenditure of available resources. The feasibility of threat elimination must be considered in light of financial, legal, and human considerations.

Threat Probability: The probability a threat will occur during the plan's life. Threat Probability may be expressed in quantitative or qualitative terms. An example of a threat-probability ranking system is as follows: (a) frequent, (b) probable, (c) occasional, (d) remote, (e) improbable, and (f) impossible.

Threat Resolution: The analysis and subsequent action taken to reduce the risks associated with an identified threat to the lowest practical level.

Threat Severity: A qualitative measure of the worst possible consequences of a specific threat:

Category 1 — Catastrophic. May cause death or loss of a significant component of the transit system,or significant financial loss.

Category 2 — Critical. May cause severe injury, severe illness, major transit system damage, or major financial loss.

Category 3 — Marginal. May cause minor injury or transit system damage, or financial loss.

Category 4 — Negligible. Will not result in injury, system damage, or financial loss.

Unsafe Condition or Act: Any condition or act which endangers life or property.

Vulnerability: Characteristics of passengers, employees, vehicles, and/or facilities which increase the probability of a security breach.

Chapter 1
Opening Pages to the System Security Plan

Chapter 1
Opening Pages to the System Security Plan

There are several opening pages you'll need to prepare before you start the actual Plan. Each will be explained in this Chapter. ***Note:*** *Please refer to the opening pages of this Guide to see an example of most of the following:*

- ○ Title Page
- ○ Acknowledgments
- ○ Table of Contents
- ○ Foreword
- ○ Management Commitment and Directive/Policy
- ○ Executive Summary (optional)

Title Page

A title page will introduce each Program Plan and should contain the following:

- ○ Name of Plan
- ○ Date
- ○ Authors
- ○ Submitted To:
- ○ Submitted By:

Acknowledgments

Give credit to all the people and organizations who contributed to the Plan or Program and express your appreciation. Show an established and working relationship with the local government and other key entities within the system's area, including municipal police, sheriffs departments, and other special forces concerned with security.

Table of Contents

The Table of Contents should list all chapter numbers, chapter titles, and page numbers. Following the chapter listings, prepare a List of Figures and a List of Tables, each starting on a new page.

Foreword

The Foreword should give a clear understanding of the Plan and how it is expected to serve as the dynamic structure for implementing an effective Program. It should include a brief expression of why the Program Plan was created and a list of objectives that have been satisfied. The Plan should

- clearly outline and discuss the process the system has identified in order to implement system security,
- define the management of the program and the roles and responsibilities of passengers, employees, and those using transit facilities such as stations, and
- identify the steps necessary to put concepts into practice and identify the evaluation program which will monitor the program and the Program Plan.

In developing the Plan, identify a list of objectives intended to be achieved through implementation. The objectives can be briefly summarized and include examples of how they are expected to be carried out. One of the objectives could be to create a new system security department, to staff it, and to appoint an experienced security professional who reports directly to the General Manager of the system. Mention briefly who that professional is and a few words on his or her experience.

Other objectives may cover identifying specific security problems which are given high priority. Such problems may include fare evasion, vandalism, and muggings. In some major cities additional problems and issues may be the impacts on security of the use of transit stations by the homeless as places to reside. Transit stations are often a location opportunity for the sale of drugs and for the initial staging of gang activities. The document needs to be specific to demonstrate a clear understanding of the problems being addressed by the Program and the fact that the system has identified actions which will improve local security.

Management Commitment and Directive/Policy

The Program and Plan must have the commitment of management. It is extremely important that the General Manager, Chairperson, Executive Director, Board of Directors, and other leaders demonstrate their full commitment. This commitment needs to be clearly stated in the opening pages of the Plan. A brief statement by top management should establish that security is integral to the operation of the system. The statement directs responsibility for security to an individual or group and indicates full support. The statement must also indicate that the Program Plan is the basis from which security roles and procedures will be implemented on a daily basis.

The following memorandum may be used as is or modified. The complete Plan should be distributed to department heads and other responsible managerial

employees. They will know exactly what is being implemented and how they and the program are expected to perform. Managers should be instructed to share limited information appropriate to the employees in their particular divisions on an as-needed basis.

Memorandum

To: All employees and other interested individuals

From: (General Manager or Executive Director)

Date:

RE: System Security

It is the objective of the (name of transit system) to provide secure and reliable service to its passengers while minimizing vandalism and property destruction associated with the (transit system)'s vehicles and facilities. To this end, it is the responsibility of all of (name of transit system) employees to make sure we provide service in the most secure manner possible.

As part of our commitment to security, the (Board of Directors or any other appropriate body) has passed a resolution calling for the development and implementation of a System Security Plan and Program whose overall goals are to maximize the level of security experienced by all passengers, employees, and any other individuals who come into contact with the transportation system, and to minimize the cost associated with the intrusion of vandals and others into the system.

To ensure that this Security Program Plan is successfully implemented, (name of individual) has been appointed the System's lead security officer. As part of this security program, employees are required to bring any conditions perceived to affect security to (the lead security officer's name)'s attention.

The (Board of Directors or any other appropriate body) of the (name of transit system) and I are absolutely and fully committed to this System Security Program Plan because it formalizes security in concert with safety as our transportation system's top priority. Please join with me in supporting this important program.

Executive Summary

An Executive Summary is optional. When used, it should give a summary of what the following pages contain. This is helpful to anyone who wants an overview and does not want to read the entire Plan.

Chapter 2
I: Introduction to System Security

Chapter 2
I: Introduction to System Security

Section I of the Introduction to the Plan will serve as a basis for presenting the concept of system security to users and to other interested people and agencies. It will include the following sub-sections:

- Summary Statement
- Purpose of System Security Program Plan and Program
- Goal, Objectives and Tasks of the Program
- Scope of the Program
- Security and Law Enforcement
- Management Authority and Legal Aspects
- Government Involvement
- Definitions Within the System Security Program Plan

Summary Statement

The Summary Statement should explain the purpose and intent of the Plan. The following is an example of a Summary Statement.

Summary Statement

To emphasize the importance of security in all aspects of our organization, (name of your organization) (herein referred to as the system) has established a set of comprehensive security activities which are documented in this System Security Program Plan. The overall goal of this security program is to maximize the level of security afforded to all of our passengers, employees, and any other individuals who come into contact with our system, as well as vehicles and facilities.

As a result of this program, the system hopes to achieve not only an improved security record but to establish security in concert with system safety as its number one priority. In order to be effective, the program documented below is oriented toward identifying potential security problems and implementing remedial and/or mitigating solutions

before security breaches can occur. In addition, this Program Plan emphasizes post-security-breach analyses so that appropriate and effective steps can be taken to minimize or prevent security breaches in the future.

The purpose of this plan is to help establish and maintain the System Security Program for the system. It serves as a blueprint for all security activities by:

- establishing how security activities are organized;
- outlining employee responsibilities with respect to security;
- instituting threat and vulnerability identification, assessment, and resolution methodologies; and
- setting goals and objectives.

This plan will be annually updated to record and evaluate past security performance of the system, to identify modifications that are needed and to establish objectives for the upcoming year. Although this plan sets a course for the direction of the Security Program to follow, the plan's existence alone does not guarantee success. A commitment by the system and all of its employees to incorporate security into every aspect of the system's operations is the only way to ensure improvement. For this reason the system's employees are considered to be the most important component of both this Security Plan and the Security Program it supports.

Purpose of System Security Program Plan and Program

Develop a plan which defines and implements the Program. If careful consideration is not given to this relationship, the Plan could become an academic exercise and wind up on someone's shelf, collecting dust.

The system should adopt a proactive, prevention-oriented approach. However, no matter how well planned and implemented security is, there will always be some security breaches which will require reactive law enforcement actions. This is expected and provisions need to be made. Current thinking regarding transit security emphasizes the importance of identifying potential threats and areas of vulnerability, developing approaches that will minimize those threats and vulnerabilities, and demonstrating a clear and proactive approach to security.

In short, "system security" means threat and vulnerability management. One of the key purposes of the Program Plan is to

- define explicitly the security roles of each person and department,
- detail their functions, and
- establish milestones for developing and implementing the Program.

Goal, Objectives, and Tasks of the Program

Goals

Readers will initially want to know what the Plan is expected to accomplish. The only goal of the Plan is to implement a Program which maximizes a system security. In this section, a set of broad system-specific objectives supporting that goal should be identified and listed. In addition, each of the objectives should have associated with it a set of very specific tasks.

Objectives and Tasks

It is important to make sure that every objective and task set is reasonable and attainable. The system should not place itself in the position of having to defend why it was unable to realize its stated objectives and tasks. This is not to say that the objectives and tasks should be trivial, but they should be well thought out and attainable. Objectives should be open-ended and able to be adjusted to changing fiscal and political situations. Tasks should be specific and should support the objective with which they are associated. For quantitative objectives, ranges should be used which provide boundaries for reasonable expectations.

Depending on the local situation at the system, the following sample objectives and tasks may or may not be useful. They may be included by those systems for which they are valuable and used as a springboard for creative thinking by other systems.

Sample Objective	Associated Tasks
To develop an information system to log all security breaches so that appropriate analysis and decisions can be effectively made.	Create a recordkeeping system that would log incidences by date, location, type, and disposition. The system should be available for on-line entry of all data. Create a data system that would have a query capability so that users can ask questions such as how many incidences of fare evasion occurred during a specific time period at specific facilities. Interface the management information system with a graphics capability so that the quantitative statistics can be expressed with bar charts, line graphs, or pie graphs.

Sample Objective	Associated Tasks
	Display the current year, along with comparable statistics for a similar timeframe, in tabular or graphical form.
To reduce the volume of a particular security breach by a certain absolute number during the coming year. (Be careful with this kind of approach since the frequency of occurrence of some breaches is really quite small in many systems. For example, there are some systems that have operated for a long period of time without the fatality of a passenger or employee. You cannot reduce the target to less than zero.)	Increase the average amount of time that passes between particular breaches. Increase the number of passengers transported between security breaches.
To equip the transit security forces in order to maximize effectiveness æ provided the transit security force does not have an adequate supply of equipment, including vehicles, communication devices, firearms, uniforms, or other items necessary to increase their capabilities and professionalism	Identify the equipment used by similar transit systems to guide the local system in its purchases. Determine the kind of vehicle which is most effective in transporting a security officer to a security breach location. Options such as automobiles, short utility vehicles (Blazers), extended utility vehicles (Chevrolet Suburbans), motorcycles, mopeds, and bicycles would be considered. The vehicles selected will depend on the characteristics of the system and its operational environ ment. Indeed, with rail systems, the most effective response mode may be by train.
To determine what transit security forces can do to increase the amount of community spirit in support of today's social issues. (For example, in some major cities, transit stations have become transient residences for homeless individuals. Policies which would require transit security officers to be sensitive to the problems of the homeless could realize benefits for the transit system.)	Identify or develop training courses which would increase the sensitivity exhibited by transit security officers during their normal duties. Evaluate what can be done by the local system to alleviate the problems of homelessness.
To encourage passengers to use the transit system more often. (There is a significant body of knowledge which suggests that if passengers perceive that security individuals are nearby, they will use the transit system more often.)	Provide standard uniforms for all security officers. Allow the security officers to participate in the selection of the uniforms. This can have the added advantage of improving morale.

Sample Objective	Associated Tasks
To make a specific sum of money available for security officers to attend specialty transit policing meetings, seminars, or conferences.	Provide competitions and awards for superior levels of performance and demonstrated involvement in community efforts.
To make the transit system much more proactive in preventing or mitigating security problems.	Create a proactive security committee made up of transit officers and community representatives charged with identifying steps to minimize security incidences. This could be designed to involve the proactive security committee in interactions with local news media to communi cate steps being taken to improve conditions. Have the committee evaluation security data. Work with the local law enforcement community and evaluate whether there are any crime patterns which could be identified.

Scope of Program

This section of the Program Plan should be designed to provide information on the intent of the Security Program, who is involved, their functions, and how they relate to the goals and objectives identified in the preceding subsection. As a short summary of major concepts, this subsection could also be used elsewhere by the transit system as an executive summary defining the role of the Security Program.

As an example, this section might state:

Scope of Program

The system is dedicated to maximizing the safety and security of all of its passengers, employees, and other interested citizens in addition to the vehicles, equipment, and facilities utilized by the system. This commitment is demonstrated by the creation of a Transit Security Division within the transit system which reports directly to the General Manager and consequently has greater access to decision making than the other line functions such as Maintenance, Operations, Accounting, Personnel, etc. The Security Division has been granted the authority to employ a highly qualified, moti-

vated, and well-equipped force of (number of) Security Officers. The Division is lead by (responsible leader), who is a career veteran of Transit Security activities and is well trained in all of the currently identified important issues within Transit Security.

The functions of the Transit Security force are to maximize passenger and employee security; minimize fare evasion, facility vandalism and destruction; and generally increase the quality of service being provided by the system.

In developing the system's Program Plan, this section should be tailored to support other materials that are included. This Security Program Plan will be required to be annually updated to record past security performance of the system, to identify modifications that are needed, and to establish goals for the upcoming year. Although this Security Program Plan sets a course for the direction of the Security Program to follow, the plan's existence alone does not guarantee success. A commitment by the system and all of its employees to incorporate security into every aspect of the Authority's operations is the only way to ensure that security experiences will be improved. For this reason the system's employees are considered to be the most important component of both this Security Plan and the Security Program it supports.

The objectives of the program can be quickly summarized in sentence form. For example, "the system is committed to regular, targeted training of the security force, the provision of adequate amounts and kinds of equipment, and to working conditions which maximize the force's effectiveness."

Security and Law Enforcement

Transit systems should take a proactive approach to security through the development and implementation of a Program and Plan. Security breaches, however, will still occur and will need to be handled. If the system relies on its own transit security forces, the Plan must explain the level of responsibility of the forces and their relationship with the local municipal police department and other law enforcement agencies. If the system depends on the municipal police department for security, the Plan should discuss how the system interacts with the police and what sorts of agreements are in place. Transit systems purchasing law enforcement capabilities from private companies or sheriff's departments should discuss in their Plan, the relative roles of the law enforcement community and security departments, and the reasons for the particular security arrangement.

Whatever law enforcement agency the system utilizes to support its security forces, that agency's primary function will be to react to security breaches. The Program Plan should specify how law enforcement and transit security personnel work together, how they communicate, and how they share jurisdictions.

It is extremely important to have, or to develop, a strong working relationship

between transit security and law enforcement forces. In a few locations, there is occasionally some friction between transit security forces and the municipal police. It is crucial that the System Security Program Plan take definite, positive strides to eliminate or prevent negative relationships.

Management Authority and Legal Aspects

The basis for the creation of the system should be defined. This section should present the system's mission statement and the information related to the extent of its specific transit-related responsibilities. If the system is chartered to maintain its own security force, or if the municipal police department must be used to provide security, the legal basis for such requirements and responsibilities should be defined.

The authority and legal aspects of management relate directly to the expected liabilities associated with the system's security role. For example, in some states, the maximum liability that can be assessed to a transit system is limited by legislation. That liability would extend to the security forces and the activities in which they are engaged. The legislation establishing the system's responsibilities should be discussed here.

Government Involvement

It is a rare transit system which can operate strictly on the revenue generated by its farebox. The overwhelming majority of systems depend heavily on federal, state, and local funds to supplement their farebox revenues. Grants from governmental agencies are always encumbered with rules and regulations which impact the operation of the transit system and, in some cases, the methods used to maximize security. It is useful include information on the sources of all major funding and to explain impacts on security that are due to the terms and conditions of the grants.

It is not necessary to include every single origin of revenue. Just categorize the source of revenue by major governmental entities so that an understanding can be quickly conveyed. For example, significant amounts of funding come from the federal government. The federal government's rules on third-party contracting regarding recordkeeping may reduce the number of security companies willing to offer security capabilities. Similarly, some transit systems receive significant grants from state departments of transportation. In some cases the amount of those grants is specific only for the year they were awarded, and a lack of continuity from year to year prevails. If revenue from a state source fluctuates dramatically each year, it is more difficult to maintain fixed levels of security. Local funds may also be irregular, yet may require that the transit security forces provide some security activities in areas adjacent to transit systems. Such services may simply be an extension of town-watch-type actions by citizens or may require the use of forces in the event of a natural emergency such as a tornado or hurricane.

The information in this part of the Guide can serve other purposes. For example, the information may be supportive of the need for a regional sales, property, or earned income tax which could provide stable and consistent funding for the system. The Intermodal Surface Transportation Efficiency Act of 1991 may also be a source of new funds for security with the opportunity to set aside monies (i.e., 1 percent of Section 9 funds).

Definitions Within the System Security Program Plan

In developing this portion of the Plan, the system should define various transit terms and a security language so that the Guide can be clear and consistent. This section can be written in one or any combination of the following ways:

- Write a narrative without being too wordy.
- Use a bulleted format.
- Write general descriptions of the various security concepts, and include more detailed formal definitions in an Appendix. An Appendix would require the reader to look back and forth between the text and the Appendix, so use this option sparingly.

Note: *Please refer to "Introducing This Guide" for a list of definitions.*

Chapter 3
II: Transit System Description

Chapter 3
II. Transit System Description

Section II of the Plan is concerned with describing the transit system to which the Plan is directed. It should be designed to stand alone as a description of the system. This section will summarize the passenger, vehicle, and facility components, the operating environment, the role of the safety plan, and existing security conditions.

The transit system description should conform to the following outline:

II. TRANSIT SYSTEM DESCRIPTION

- A. Background and History of Transit Agency
- B. Organizational Structure
- C. Human Resources
- D. Passengers
- E. Transit Services/Operations
  (Fixed Route Bus, Commuter Bus, Light Rail, Commuter Rail, Subway, Paratransit, Other)
- F. Operating Environment
  - 1. Traffic
  - 2. Weather
  - 3. Geography
  - 4. Crime Rates
  - 5. Other
- G. Facilities and Equipment
- H. Passenger, Vehicle, and System Safety Plan and Program
- I. Current Security Conditions
- J. Existing Security Capabilities and Practices
  - 1. Proactive Measures
  - 2. Response Measures

The Plan will be of interest to many people, not only those familiar with the system. Although the Guide should be designed as a working document, it may also be used as a reference by the general manager, security manager, driver supervisors, board members, city planners, non-transit police, citizens' interest groups, and government officials. Readers who are and are not familiar with the transit system should be able to use the Plan to understand the nature of security within the transit system.

The inclusion of systemwide information in the Plan lends a clear indication that security is an integral part of transit operations. It is important that security should not be considered a separate program by employees, as maintenance and operations staff sometimes feel about their own departments. Further, this helps those responsible for planning to address every aspect of the system in developing and reviewing security policies.

The inclusion of a comprehensive description of the transit system is not unique to a Plan. Passenger, Vehicle, and System Safety Plans, annual reports, ADA Complementary Paratransit Plans, and other formal documents also require such a description. This material should not need to be developed from scratch. If it is necessary to generate completely new material, the description or parts of the description may be used for other documents. The history of the transit system, for example, is unlikely to change from one year to the next. It is not necessary to concentrate solely on security in this section. Security will be the prime concern of all other sections of the Plan.

The specific contents of the transit system description will naturally depend upon the system itself. However, there are a number of topics that should be addressed. Before developing this section of the Plan, remember that the Plan is being developed with a systems approach. As you will recall the definition of a system is:

> A composite of people, property, environment, and procedures that are integrated to perform a specific operational function in a specific environment.

The system description will be comprehensive. The elements of a system, shown in Figure 3-1, are diverse and interactive. Consider this big picture and the myriad of potential audiences as the description of the transit system is developed.

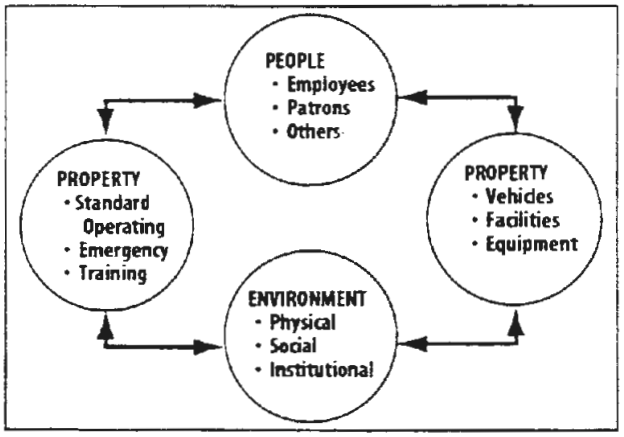


Figure 3-1.
Elements of a System

A. Background and History of Transit Agency

Give the reader a clear picture of the evolution of the transit system and its place in the community. It should open with a brief summary, followed by a chronological order, beginning with the original need for transportation services and the empowerment of the transit system. Indicate when the system was empowered, how it was empowered, its history of service delivery, and major milestones that have been accomplished, such as expansion into new transit modes. A brief indication of passenger volumes may be included.

The transit system description should be in concert with the level of detail shown in the rest of the Plan. For a small system, the background and history can be a single page without a summary introduction. For larger and older systems, longer backgrounds may be appropriate, in which case a summary introduction should be included. The introduction may consist of a single paragraph that summarizes the history and background subsection, such as the example that follows:

> The Bus System was empowered by the state legislature in 1939 and charged with the responsibility of efficiently providing all public transportation services within the corporate limits of the City. As the City grew, the transit system also expanded. The name of the system was changed in 1954 to reflect its greater role as the City Transit system, and today operates fixed routes, a park-and-ride service, an express/commuter service, complementary paratransit, and one commuter rail line.
>
> **or**
>
> The transit system is the product of a federal-state-local cooperative relationship dating from the late 1960s and early 1970s when local private bus companies were struggling to stay in business due to rising inflation, escalating fuel prices and decreasing ridership. By authorizing the system to acquire the assets of several private companies, the state legislature and admini-stration assured the public that buses would continue to run in the state's capital. Transit service in the City is believed to have begun before the Civil War, when a horsecar route operated between the thriving port of the Town and the Navy Yard. A brief look at the transit service of the past follows.

B: Organizational Structure

Include an overall organizational chart and define the various functional portions of the transit system administration. Specific details on the security and safety portions of the structure should also be included. For the sake of clarity, the organizational structure should begin with the role of the transit system. It should then describe and show the relationship of the system to its

governing bodies. If the system, or its general manager or executive director, reports directly to a board or a state Department of Transportation, note that. For example:

Governor of State

Hon. R. Smith

|

Department of Transportation

|

TS Board of Directors

|

The Transit System
Executive Director

Next, the overall structure of the transit system should be described. Include both an organizational chart and a narrative. In this subsection of the plan, it is the organization that is important, not the actual individual. Describe the organization of departments, making clear the chain of command among departments. For example, what is the organizational relationship between Maintenance and Operations? It maybe helpful to think in terms of who reports to whom, and then translate that into functions.

Some departments report directly to the general manager or another key manager without specific line authority over all departments, offices, and personnel under that manager. Many executive directors prefer to have a security officer work directly through them. Such organizational nuances should be reflected in the organizational chart and narrative. The organization of the entire system should be included, but the functions specific to security may be highlighted to customize it for the Plan. The narrative should specifically address the role of Security departments within the system.

The organizational chart for a small or rural system may be as shown in Figure 3-2. A typical large transit system organizational chart is shown in Figure 3-3.

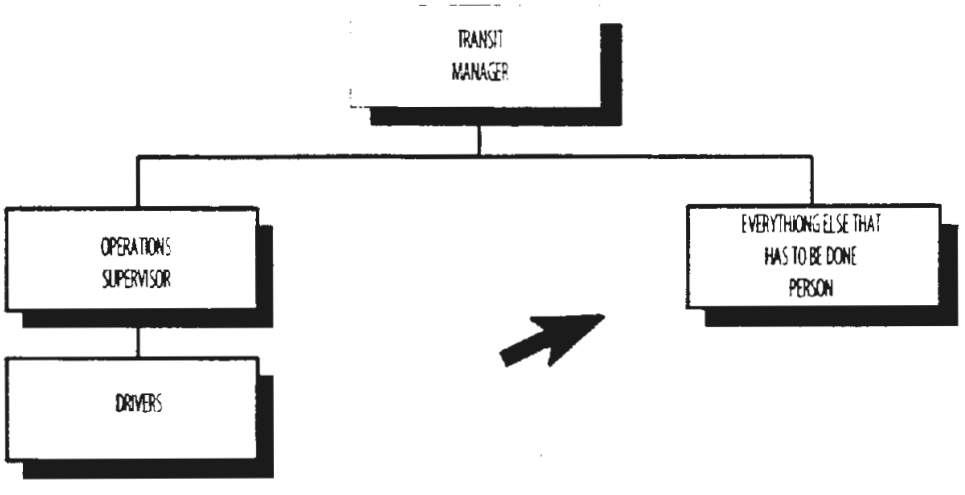


Figure 3-2. Sample Organization Chart for a Small or Rural System

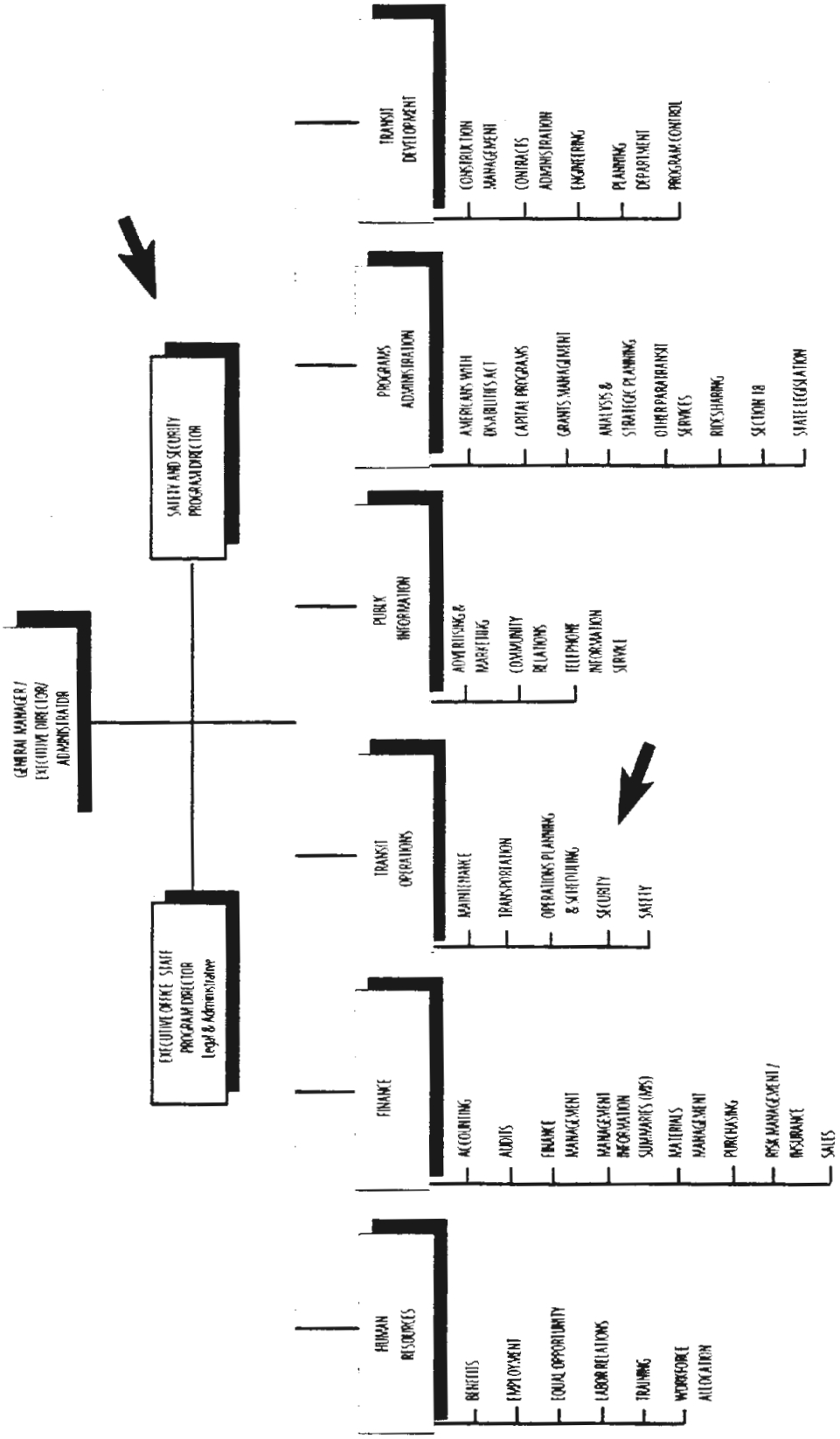


Figure 3-3.
Sample Organization Chart for a Larger System.

C: Human Resources

The key to a Program is the group of people who make up the transit system. As the organization of the transit system has been explained, this subsection should focus on the staff. It should contain a summary of the number of employees, their various disciplines, and how they are divided among the various functional entities within the system. This information should be brief. Transit security should be an aspect of every employee's job, and this approach should be reflected here. It would be appropriate to explain that every employee in the system has at least one security-related responsibility shown in his/her position description.

Describe the special skills that members of the organization have that are relevant to security, such as degrees in law enforcement, the experience of staff in security, or special training. Describe also what relationships the system may have with security experts and resources outside of the organization. Special attention should be paid to the relationship of the security officer or group to the rest of the transit system and to other organizations. The following chart may assist you in doing so:

Interfaces of Security Officer/Group with Other Departments and Organizations

Department/Organization	Security Relationship
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.
6.	6.
7.	7.
8.	8.
9.	9.
10.	10.

D: Passengers

In order to understand both the transit system and its security needs, it is important to know about the passengers it serves. Included in this section will be graphic and narrative representations of passenger demographics, grouped by travel mode or other characteristics. Both population and ridership information should be included, as they are important to the Plan. This Summary information, however, should be brief. An appendix may contain additional information on population and ridership. Separate population and ridership documents should be referenced. This subsection of the Plan may first discuss the general population of the area served. The total population should be presented first, after which the Plan may break that population down by service area. The Plan may use a format such as follows:

The System, serving the greater part of (general area served), serves a total population of (latest census figure). These residents are distributed among the several communities served, including (community A), (community B), and the surrounding county (or metropolitan area), as shown below:

	Population:
Community A	10,000
Community B	9,000
Surrounding (Area)	31,000
(Total service area)	50,000

Substitute whatever political boundaries or census areas may be applicable to the transit system.

Additional demographic information, such as age and socioeconomic information (based on the latest census data) may be useful in understanding the public which the transit system serves. If so, include that information here in a simple format.

Ridership information must also be described. Introduce the ridership information in narrative form, describing the number of passengers carried per year and any superlative information that may be interesting or applicable. If such information is available, describe where or when most trips are taken. The Plan should mention whether ridership is growing, stable, or declining. A breakdown of ridership information in tabular form should be included but should be kept relatively simple, showing one-way trips by community of origin if available:

1993 One-Way Trips

Community	All Modes
(Community A)	_____
(Community B)	_____
(Community C)	_____
Total	_____

Many transit systems that receive federal funding through Section 15 grants regularly report ridership data in standardized formats. This information may be inserted here. It is appropriate to describe ridership by time of day and day of the week as this will impact security needs. Refer the reader to other sources of information if necessary.

E: Transit Services/Operations

Introduce the various modes of travel services provided by the transit system and the summary information about the amount of exposure they face. For each applicable mode (fixed-route bus, commuter bus, light rail, commuter rail, subway, paratransit or other mode), a summary of the various routes, the

volume of trips delivered, and other statistical information should be provided. With regard to each mode, a short description should precede any relevant tables. The following information may be communicated:

- total number of routes
- volume of trips delivered
- start-up date
- major changes expected in the next year
- total number of security-related incidents
- service area
- total budget
- any unique service characteristics

Following the introduction of each of the modes, the Plan should present operational characteristics which reflect the amount of exposure the transit system experiences on a daily basis. This exposure information is valuable to the reader and planner alike in that it establishes the difficulty of protecting operations. Most of these operational characteristics can be expressed in terms of hours. For each transit mode include

- the days and hours of service provision,
- the total number of hours each mode is exposed per day, (Every hour that each bus or other transit vehicle is not parked in a secure area is an hour of exposure; for example, 100 buses operating 10 hours each will represent 1,000 hours of exposure.)
- the total number of vehicles owned and the total number used at peak-hour, and
- operational characteristics such as traveling in the mountains during snowy or icy conditions, which reflect the amount of exposure the transit system experiences daily.

Conclude with a brief reference to separate documents such as public brochures and annual reports that contain additional information on transit services.

F: Operating Environment

Briefly present narrative information about traffic, weather, geography, crime rates, and any other characteristics that describe the local environment:

1. Traffic: A description of the level of congestion and volume of traffic associated with the roadways and guideways in the service area. This will not be specific to particular routes. It will be systemwide in description.

2. Weather: A paragraph indicating the type of weather patterns within the region in which the transit system operates.

3. Geography: A paragraph summarizing geographical features of the service region. Discuss anomalies or designs which cause or solve problems. For example, major rivers in the service area can often inhibit movement to available bridges. In contrast, transit applications such as timed-transfer operations in the central business district can often improve the quality of service related to the area.

4. Crime Rates: A paragraph summarizing crime rate information for the areas which the system serves. Crime statistics are available in various levels of detail for most urban areas and may become an integral part of Program planning. Only city-wide statistics, totals, and trends in crime rates should be reflected here.

5. Other: A paragraph describing any other characteristics within the local environment which may have an impact on security and/or safety.

G: Facilities and Equipment

It will be necessary to provide appropriate information on the various administrative and garage facilities and equipment owned and operated by the transit system. Each of the facilities should be discussed. Include information on their location, function, square footage, number of employees, etc. This information should be presented in a narrative description of the facilities and should be accompanied by summary tables. For example, the table format shown in Table 3-1 may be used as is or as the basis for the system's presentation.

Facilities and Equipment

Name of Facility	List of Buildings	Square Footage Associated with Each of the Identified Buildings	General Function of the Overall Facility	Specific Functions Associated within Each Building of the Facility	Number of Employees Associated with Each Building within the Facility	Description of Security Devices Utilized (for example, 6-foot chain-linked fence, 6-foot chain-linked fence with barbed wire, 6-foot chain-linked fence with razor wire, 8 foot chain-linked fence, etc.; closed-circuit TV, burglar alarms, motion detectors, armed or unarmed guards, dog patrols, etc.

Table 3-1. Facilities and Equipment

The tabular data should allow the reader to fully realize that each of the facilities has its own set of characteristics. Table 3-1 can be expanded to include the equipment maintained within the facility or separate tables can also be used. It is helpful to know how many exits are associated with each building, whether there are windows, what types of rooms are included, and whether storage areas exist.

In addition, detailed information related to the maintenance of security at each of the facilities should be included. Information on alarms, cameras, and other security equipment would be useful. Also include information on the hours of operation of each facility and the hours during which only security forces or devices are present. This information may be useful in the development or analysis of specific collected data. For example, the effectiveness of closed circuit television (CCTV) equipment may be examined by comparing the volume of instances of security breaches at facilities with CCTV to those without.

H: Passenger, Vehicle, and System Safety Plan and Program

Aside from this Plan and the Program it presents, the system should also have a Passenger, Vehicle & System Safety Plan and Program. In many ways, safety and security comingle as significant concerns of the transit system. Over several years, the FTA, through its research arm, the Volpe National Transportation Systems Center, has recommended that each transit system put together a Plan and Program. The Plan and Program should be a companion volume to the Plan and Program.

The fundamental difference between safety and security was discussed in the Introduction to System Security section.

- Safety is freedom from *accidental* danger.
- Security is freedom from *intentional* danger.

The Plan should discuss how to be prepared with a proactive approach to preventing or mitigating accidental dangers. Overall, the approach should prevent potential safety problems before they develop and should prepare the transit system to react to safety issues when they actually occur.

The structure of the Plan should be very similar to that of the Plan, except that the concerns here are not with accidental situations, but with deliberate actions taken by perpetrators to acquire money, goods, or equipment or to deliberately damage or destroy equipment and facilities. The Plan should also be very concerned about minimizing the number of attacks or assaults on passengers, employees, and others using the system.

This subsection of the Plan should summarize the overall philosophy of the Plan and Program and integrate it with the Plan and Program. Some of the individuals on the proactive safety committee may also be members of the proactive security committee, which is discussed later in this Guide. Similarly, those individuals responsible for analyzing safety statistics and developing conclusions about how

safe a facility or system really is may be quite effective in accomplishing analyses related to security.

A significant difference between the Plan and the Plan is that the security forces may not be employed by the system. They may be under a service contract with the system and provide security through a separate, private, for-profit company or a municipal police department. The system should clearly demonstrate the similarities and differences between the two types of plans and programs.

I: Current Security Conditions

The Transit System Description section of the Plan should develop a portrait of the current conditions. (Up to this point, information should have been on the facilities, the people, the equipment, the service, and other information designed to convey a perception of the system.) In this subsection, it is important to summarize the kind of security breaches that have occurred within the system to date. Include documentation on the frequency of problems experienced during the previous one-, two-, three-, four-, or five-year period. Examples of security breaches may include, but are not limited to:

- assault and battery
- bomb scares
- computer database intrusion
- disorderly conduct
- domestic threats
- drug abuse
- drug sales
- exhibitionism
- facility and equipment damage
- fare evasion/dodging
- forgery
- fraud
- graffiti
- vandalism
- lewdness
- muggings

- personal crime
- property crime
- rape
- revenue theft
- sabotage, destruction and altering
- stock/parts shrinkage
- solicitation
- strong-arming
- terrorism
- theft
- trespassing

The system may choose to use this list to classify security breaches or it may choose to use its own categories. It may also choose to include only those security breaches which actually occurred, along with their frequency of occurrence. Alternatively, the system may want to develop a comprehensive list of security breaches and demonstrate, in a frequency of occurrence table, that it is free of some of the security problems experienced by other transit systems. It may be useful to contact other transit systems in the system's state or the state transit association (if one exists) to determine what lists of security breaches are available.

By identifying problems experienced by similar transit authorities that could arise locally, the system prepares itself to address potential security problems. This information will be useful later when you compare the experiences of various transit systems for certain periods. It can also serve as the basis for statistical analyses which can be used to identify specific goals and objectives. Each existing security problem and proactive measure being considered should be discussed.

J: Existing Security Capabilities and Practices

Summarize what is currently being accomplished by the system to maximize security provided to passengers, employees, vehicles, facilities, and equipment. It may include a discussion of devices and procedures currently used.

A strong emphasis on proactive measures is needed. However, since security is freedom from *intentional* danger, the perpetrators can be expected to be successful sometimes. The response measures (law enforcement) currently employed by the transit system should also be summarized here.

1. Proactive Measures

This subsection should include a summary of the existing methods and procedures, devices, and systems that currently exist to prevent or minimize security breaches. They may include committee work, analysis, training programs, and passenger coaching. For example, the system may have created a proactive security review committee responsible for identifying potential and existing problem areas, developing standard operating procedures, and installing various devices to mitigate or prevent breaches from occurring. If the proactive security committee has been asked in previous periods to address certain issues, those measures should be included here.

If the system has developed databases on the various security breaches which have or could occur, then the analysis of that collected data, the conclusions drawn, and the activities that have been implemented to improve security should be discussed.

It is reasonable to assume that the system has taken steps to provide training for its employees. Training might include the development of psychological, physical, and behavioral profiles of passenger attackers so that those individuals can be high on the target list for surveillance activities.

Most employees become overly familiar with their own work environment and cannot recognize its faults. It may be worthwhile for the transit system to conduct peer security audits as part of the training program. The system would visit the facilities of other transit systems within the state, nearby, or at properties of similar size, and conduct a detailed security audit. Once the audit is completed, a presentation of the findings to the local system could identify significant threats and vulnerabilities which would need to be remedied. Once trained, transit security personnel from different systems can benefit each other with practical and classroom training on the identification of vulnerabilities.

Also included in this section should be:

- Information on any and all training courses which have been completed by system personnel and resulted in an increased proficiency in security.
- Any passenger coaching the system has accomplished. (This may include exhorting passengers through advertising on buses, subway trains, and stations to closely guard their purses and wallets or to avoid wearing chains, earrings, or other jewelry which could easily be a target for snatching; to never exhibit large sums of money; to avoid standing in dark, remote locations in transit centers; and to maintain a general awareness of the surrounding environment.)
- Use of intrusion alarms, motion detectors, and other devices on facility entrances.
- The proactive value of closed-circuit television systems (if used) and publicity indicating their presence.

While many law enforcement activities performed by police departments tend to be reactionary in nature, the system should endeavor to include the law enforcement community in proactive, preventative activities. If the system has involved the police department, then a description of those activities and the benefits realized should be discussed here.

2. Response Measures

No matter how proactive the system is, there will still be some security breaches. Moreover, the transit system's security forces may respond to security breaches. It is highly probable that local law enforcement officers may end up having greater authority at the scene. The hierarchy of authority should be discussed here, along with the method for communicating with law enforcement when a security breach occurs. The capabilities and practices of the local law enforcement agencies with respect to how they currently respond to security problems within the transit system should be discussed.

Standard operating procedures for notifying transit security forces that a security breach has occurred need to be discussed, and the role of transit security officers when they arrive on a crime scene needs to be explained. It is extremely important that the Plan clearly detail the jurisdictions of each of the various law enforcement groups, including both the hierarchy of decision-making and the level of responsibilities.

Chapter 4
III: Management of the System Security Plan

Chapter 4
III: Management of the System Security Plan

Section III of the Plan provides a description of how the transit system will manage the Program. No matter what size or structure the transit system is, the Plan should account for each of the following management functions:

- Developing the mission statement and overall system security policy
- Managing the Program
- Assigning specific responsibilities to staff within the transit system
- Establishing a Proactive Security Committee
- Establishing a Security Breach Review Committee

The Management of the Plan should conform to the following outline:

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

Because transportation organizations vary in size, scope, and management structure, it is not practical to set forth the appropriate distribution of responsibilities in this Guide for all transit systems. For example, in a small system there may be one individual who is responsible for developing the mission statement and managing the Program on a daily basis. As another example of the variations in program management, the same individuals may serve on both the Proactive Security Committee and the Security Breach Review Committee. However, large urban systems could have separate committees (or subcommittees) for these functions for each transit mode.

A: Responsibility for Mission Statement and System Security Policy

A successful Plan requires leadership from the top down and involvement at all levels. This part of the Plan should identify the individual or group that develops (and signs) the mission statement of the Plan. In most cases, that will be an executive director, managing board, or some other top-level manager. The plan should emphasize the importance of the mission statement in setting the tone and emphasizing the priority that management places on system security.

System security policies may be the responsibility of the same executive director or managing board. This part of the Plan will identify the individual or group responsible for setting the transit system's security policies. Depending on the operation of the Program, policies may be developed cooperatively with local law enforcement agencies. In larger transit systems, legal staff may be involved in developing the system security policies. The Plan should relate the development of security policies to the overall mission of the Program. The individuals responsible for revising existing security policies should also be identified in this portion of the document.

B: Management of the Program

In general, there are two basic structures for managing a Program:

1. In smaller systems, the transit system manager has many responsibilities, which include overseeing the Program and carrying it out on a daily basis.

2. In larger systems, the transit manager is ultimately accountable for system security but is more removed from daily operations. Therefore, it is likely that another individual would coordinate the daily activities of the Program.

State which of these two management structures the transit system uses for its Program and present the general reporting and communication responsibilities regarding security issues for the entire organization

The Plan should assign these nine management activities:

1. Being ultimately responsible for secure transit system operations

2. Communicating security as a top priority to all employees

3. Developing relations with outside organizations that contribute to the Program

4. Developing relations with investigatory agencies such as the National Transportation Safety Board

5. Listening to and taking appropriate action on all security concerns brought to the attention of the appropriate individual or group.

6. Identifying potential security concerns in any part of the transit system's operations

7. Actively soliciting the security concerns of other employees

8. Serving as a liaison between the Proactive Security and Security Breach Review Committees and transit system employees

9. Working to ensure that the Program is carried out on a daily basis

In a smaller transit system, the manager would handle all of the security management activities. In larger organizations, there may be a lead security officer who is responsible for carrying out the program. This individual would concentrate on activities 5 through 9. The system manager would generally take responsibility for activities 1 through 4.

When a transit system is preparing its Plan, it may discover that its current management structure needs revising. If so, the new structure should account for the responsibilities related to the Program.

C: Division of Security Responsibilities

Earlier sections of the Plan introduce the organizational structure of the transit system and its individuals. This portion of the Plan should present a complete listing of all line and staff positions within the organization, along with their respective security responsibilities. The plan should start on a new page for each function to allow for easy revisions and additions as responsibilities change, new responsibilities come up, or jobs are created or merged. The Plan should also include a graphical depiction of the organization showing chains of command and lines of communication.

For each position, the Plan should:

- Summarize the overall security responsibilities
- Place those responsibilities in the context of other work activities
- Include a list of security-related tasks

For example, a description of the security responsibilities of a transit system's supervisors might look like the following:

Supervisors are responsible for communicating the transit system's security policies to all employees. For this reason, supervisors must have full knowledge of all security rules and policies, but more importantly, they must communicate those policies to other employees in a manner that encourages them to incorporate security practices into their everyday work. The specific responsibilities of supervisors under the security plan include:

- having full knowledge of all standard and emergency operating procedures
- ensuring that drivers make security a primary concern when on the job
- cooperating fully with (name of transit system)'s security program regarding any accident investigations
- listening and acting upon any security concerns raised by the drivers
- reporting to the security officer or the manager any security concerns.

D: Proactive Security Committee

The Proactive Security Committee is one of two committees that a transit system should establish to handle security issues. The major task of this Committee is to identify and neutralize potential security risks that the transit system may encounter — to eliminate security problems before they happen.

This Committee should conduct systemwide security assessments and make sure that new procedures and facilities incorporate security in their design. This Committee may also develop and review training programs geared to security. Members of this Committee should also look for new techniques that will improve the security of the transit system.

The Proactive Security Committee is also responsible for security reviews. These reviews

- determine compliance with management policies, rules, regulations, standards, codes, procedures, and assigned security responsibilities; and
- identify organizational issues that may contribute to recurring security incidents or less effective responses to incidents.

Moreover, this Committee may actively promote improved safety in the transit system. Activities in this area include security awareness campaigns, awards programs, and special security-related events.

The people who serve on this Committee should represent both the transportation organization and the local community. Five to seven members would allow

the Committee to have a broad representative base and to retain manageability. Small organizations may wish to have only three members on the Committee; however, this would increase the workload for each member.

Representation on the Committee might include

- individuals from various parts of the transit system and independent representatives
- dispatchers, drivers, and mechanics (if applicable)
- representatives from the local police department
- local officials
- insurance representatives (assuming they have no financial ties to the transportation organization)
- board members
- leaders of community organizations concerned about local security.

In some small transit systems, the system manager serves on the Committee. In larger systems, the head of operations may assume the responsibility of representing management. In either case, the management representative has dual responsibilities. The first is making sure that management's interest in providing a secure environment for passengers and employees is represented. The second is maintaining a sense of fairness throughout the process.

The Proactive Security Committee should meet at least once a month to work on Program issues. At the meetings, members should report security-related concerns, review potential problems, and designate members to investigate security issues. Once a security concern is brought to the attention of the Committee, one or more representatives should be chosen to evaluate the potential problem. They should then report their findings at the next meeting.

E: Security Breach Review Committee

The Security Breach Review Committee is the second of the two committees that a transit system should establish to handle security issues. The major purpose of this Committee is to identify the security breaches against the transit system and to investigate these incidents to understand the deficiencies in the Program. While the Proactive Security Committee should seek to prevent security breaches, while the Breach Review Committee looks at incidents and breaches that have already happened.

In smaller transit systems, the two committees may be combined as a single Security Committee. If possible, the transit system should create two independent committees that cooperate to share information and findings as well as to avoid conflicts of interest.

The incidents and breaches that the Security Breach Review Committee investigates may be controversial or sensitive. They may involve violence, criminal activity, or wrong-doing by members of the transit staff. Therefore, the Committee members must be viewed as impartial and above suspicion. The Committee should include members of management and non-management, plus independent members from outside the transit system. The outside members could be from the local police, municipal government, fire department, or some other organization familiar with security issues. These outside members must be objective individuals who are trusted by management and other employees.

The Committee members should review security incidents to determine whether the breach occurred because of

- incorrect policies or procedures
- procedures that were not carried out by staff
- an accepted risk
- unforeseen technology or action against the transit system
- some combination of the above

In some cases, the Committee may be able to recommend specific actions to prevent future security breaches of a similar nature. At other times, the Committee may refer the security breach to the transit system manager or the Proactive Security Committee and ask them to develop preventive measures. The Committee may also recommend cooperation with local law enforcement for incidents that the transit system cannot handle on its own. The Plan should spell out the extent of the Security Breach Review Committee's authority in recommending actions and/or changes in security policy.

Chapter 5
IV: System Security Program—Roles and Responsibilities

Chapter 5
IV: System Security Program — Roles and Responsibilities

Individuals throughout the transit system will accomplish the overall security goals and objectives if they are assigned roles and responsibilities in the form of procedures. Outline the regular security activities of the transit system. All of the tasks necessary to accomplish the goals and objectives established earlier in the Plan will be assigned to specific individuals and groups, thus creating a comprehensive working document.

In order for a transit system to be secure, priorities must be established as a general goal with specific supporting objectives. Each of these objectives must be translated into specific tasks. Everything included in this section must meet the goal and objectives established in the Introduction to System Security. It should include the tasks, subtasks, and methods by which the goal and objectives will be accomplished. If a task must be accomplished but does not meet a specified objective, the objectives must be revised.

This section of the Plan (along with the sections on Threat and Vulnerability Identification, Assessment, and Resolution, and Implementation) are the core of the Plan. Other sections of the Plan address the management, implementation, and revision of the Plan. They divide the general responsibilities among the transit staff. It is this section and the next section that should establish the ways in which all necessary components of an effective Program will actually be carried out.

The plan should account for each of the following:

IV. System Security Program:
Roles and Responsibilities

A. Planning

B. Proactive Measures

C. Training

D. Day-to-Day Activities

Be very specific and include tasks, assignments, standard operating procedures, and emergency operating procedures. The level of detail with regard to actual procedures means that the Plan will have to be kept open and revised. The transit system must be willing to update the Plan as ongoing activities change.

Combine those activities already being conducted (as long as they address the security goal and objectives of the system) and those yet to be implemented. If a full Program is not already in place, many activities will concern preliminary threat identification and assessment and known security problems. Once a Program has been in place for some time, changes to roles and responsibilities should generally be the result of the threat and vulnerability identification, assessment, and resolution process described in the following section.

Each task must be assigned to a specific person who will be responsible for accomplishing the task. This aspect of the Program cannot be emphasized strongly enough. *"Roles and Responsibilities" is the title of this section rather than "procedures," to stress the need for people to take responsible action.* If the Plan consisted of procedures only, there would be no guarantee that any tasks would be carried out or that any objectives would be accomplished. To further ensure the accomplishment of security tasks, the Plan should refer to specific individuals by title and by name. Although this will sometimes require a revision of the Plan, turnover should be less frequent than the need to revise security procedures.

An appropriate introduction to the Roles and Responsibilities section should be included, as this section will be of particular interest to the system's employees. An example might be:

> **Introduction**
>
> To ensure that operations are conducted in the most secure manner possible, all transit system personnel have been assigned specific security responsibilities. In addition to their responsibilities under the System Security Program, all staff are required to carry out their regular responsibilities as assigned and adhere to the security operating procedures described herein.

A: Planning

Outline all security planning activities and assign those functions to individuals. After the development of the initial Plan, most planning activities will either be ongoing or will grow out of the process (described in the next section) of identifying, assessing, and resolving security threats and vulnerabilities. The general process for both types of planning activities should be described and assigned here. Regular planning activities might include:

- meeting with the local chief of police annually to discuss long-term issues,
- reviewing the success of the Proactive Security Committee,
- establishing monthly security planning meeting with managers, or
- soliciting ideas from all staff for improved security.

At a minimum, a procedure must exist for developing and modifying the Plan. This responsibility may be assigned to the General Manager or lead security officer. Summarize the procedure and responsibility briefly here. The implementation and evaluation of the Program Plan will be discussed in greater detail in Chapter 7.

The transit system's Board of Directors will play a role in the planning of security activities by way of approving the initiative to develop a security plan and through review and approval of the actual Plan. The lead security officer should submit the Plan to the Board following its annual revision. In the case of a new Plan, it should be submitted after it has been finalized but before it has been implemented. The review of the Plan will ensure that the role of security is appropriate and supported. It should be made clear that the Board can also assist in the Process by communicating any particular security concerns to top management. Security might be placed on the board's agenda at least at a regular interval.

As indicated throughout the Plan, general planning responsibilities will probably be delegated to the General Manager or lead security officer. That general planning function should be stated explicitly here. The lead security officer might also have such planning responsibilities as:

- assisting the General Manager in the overall development of the Plan, writing specific portions of the Plan,
- coordinating with other departments in the establishment of security procedures,
- serving on the Proactive Security Committee.

Other managers and supervisors have a wealth of information on the operation of the transit system. They should be consulted by the security staff and security committees if they are not already members. In addition, managers should be responsible for reviewing the draft Plan, providing input on the implementation process, soliciting security concerns and suggestions from staff, communicating appropriate issues, and considering security in their normal planning activities. Such security planning functions should be clearly outlined here.

All other staff members can assist in security planning by sharing their security concerns and ideas for improvement either through a supervisor, suggestions box, or appropriate security staff. All staff members can assist in up-to-the-minute planning during the accomplishment of their own day-to-day functions. For example, all staff, drivers especially should be charged with the task of **"Considering the security of transit passengers, employees, vehicles, and facilities at all times."** Drivers and mechanics should be made aware of the importance of their own planning roles. For example, a driver must consider the security of the passengers whenever leaving the vehicle and correctly interpret and apply all standard operating procedures. The planning tasks and assignments that follow are examples. When this section of the Plan is developed, each conceived planning task should be appropriate to the

transit system and assigned to a specific person. Subsections may be organized either by task or by staff position, so that if such a list were presented, each line would be followed by the title (and preferably the name) of the responsible members of the transit staff.

Planning Tasks and Assignments

- Review new security activities to determine how they will impact the areas for which each manager is responsible.
- Develop implementation strategies for new security-related activities to be assigned.
- Develop time lines for implementation of new security subprograms.
- Consider security aspects in all new equipment acquisitions.
- Plan fiscal requirements of security activities.
- Plan for the limited distribution of keys and access to transit facilities.
- Consider the security of transit passengers, vehicles, and facilities in the accomplishment of all regular activities.
- Offer suggestions for the improved security of transit passengers, vehicles, and facilities.
- Staff the security department.
- Determine training needs for security-related activities.
- Review System Security Program Plan.
- Develop resolutions for security problems identified.
- Determine equipment requirements for all new or considered security activities.
- Meet with local police chief biannually to discuss long-term security issues.
- Review the success of the Proactive Security Committee.
- Solicit ideas from all staff on improved security.

B: Proactive Measures

Proactive security measures are those subprograms or activities undertaken to prevent breaches in security or to minimize threats and vulnerabilities. Proactive security measures rarely include activities designed to respond to security breaches unless those activities will reduce the severity of the incident during its occurrence or actually prevent future breaches in some way.

Proactive security measures should be developed at the time the Plan is written in order to address all security problems that have been discovered, especially in the case of the first Plan. Other proactive measures may have been recommended for implementation by the Proactive Security Committee or may have been only recently implemented. As the system will not always want to wait until the next Plan revision to implement proactive security measures, some may be in full swing by the time of the update. Regular proactive security measures should be shown in the Plan as usual activities. This subsection should briefly describe the problem each

proactive security measure is designed to mitigate, referencing other reports as necessary, along with the proactive measure. For each, the responsibilities for the proactive security measure should be assigned. Proactive security measures that establish new operating procedures may reference those standard (or emergency) operating procedures as presented in day-to-day Activities. Proactive security measures that need to be implemented should also include the tasks necessary to initiate the new measures.

For instance, a new proactive measure might be to require bus keys that cannot be easily duplicated. The task of writing this requirement into all new procurement bid packages might be assigned to the maintenance manager and a procedure established for running certain purchases through a security department check.

As presented in this subsection, this proactive security measure might appear as follows:

Bus Keys

The Proactive Security Committee has noted that a number of drivers have expressed concern about leaving their vehicles unattended during mandatory breaks at the end of the line. In the interest of preventing theft or damage to the buses, vehicles will henceforth be purchased with key-controlled ignitions, rather than the simple push button start used previously. These keys shall be of non-duplicable shape.

Assignments: The task of writing these requirements into a new vehicle procurement bid package shall be assigned to the maintenance manager. In addition, certain acquisitions shall be reviewed by security staff prior to purchase.

Implementation:

- Maintenance manager will consult vendors prior to the next vehicle acquisition process to determine available key configurations.
- Maintenance manager will develop standard language to be included in vehicle specifications.
- General Manager will obtain budgetary approval and include extra costs in annual budget.
- Operations staff will develop key assignment procedures for shift start, driver replacements, breaks, and lost keys.
- Standard Operating Procedures for key assignments will be amended and included in the Security Plan.

C: Training

Security training should be established for all personnel. At a minimum, all employees should be given enough training to carry out the security responsibilities expected of them. Training may range *from* ensuring that security is discussed during all regular training programs *to* sending staff members to national meetings to attend sessions on transit security.

Describe all training conducted in the interest of increased security, whether proactive or responsive. All types of training should be referenced, including new employee orientation, training requirements for security personnel, special workshops, and any training to implement new proactive measures. A single paragraph may be used to describe each training activity, although certain overall training activities may be grouped categorically. Each description should reference other appropriate documents; for example, a description of a passenger relations course for drivers might refer to the instructor's manual.

New employee orientation training is recommended for all transit personnel and should be described here. This type of training might emphasize security through a short talk by the General Manager. Security responsibilities should also be stressed in the review of each new employee's job description and appropriate operating procedures which each employee normally receives. Procedures that are more critical or complicated should be practiced.

All drivers should normally be trained in passenger relations to establish smooth operations and rapport between drivers and passengers. Passenger-relations training should address the handling of passenger problems, both harmless and security threatening. A paragraph describing such training might read:

> All vehicle operators are trained in *Passenger Relations*, a course taking one full day including breaks and exercises. In addition to covering normal company policies and how to assist passengers, the course emphasizes the need to maintain polite control of activities in the vehicle for the security of passengers and the vehicle, and covers the handling of the following:
>
> - radio playing
> - expired transfers
> - fare evasion
> - use of rear doors
> - writing on walls and seats
> - threats
> - passenger requests for assistance
>
> The specific contents of this training are detailed in the *Passenger Relations Instructor's Manual* and the *Operator's Manual for Passenger Relations.*

Professional development training (such as attendance at security workshops by lead security staff) should also be described. A transit system might, for example, send both the General Manager and the lead security officer to annual regional transportation conferences, expecting each to attend at least one workshop on security. Staff development training for operators might include scheduling yearly drivers' meetings at which the local police talk about the role of citizens and transit operators in the handling of serious incidents.

Some detail should include a description of training for the security staff or the training required of new hires for the security department. Some systems require specific training from a certified academy; others require that certain tests be passed during pre-employment screening. Many also conduct on-the-job training of security staff.

Describe all new training required to implement the new proactive training measures previously described. The training will change to reflect the newest proactive measures each time the Plan is updated. These training areas may be described as one time, such as the training of supervisors in the use of closed-circuit television monitoring equipment when the equipment is installed, or the inclusion of vehicle lock-up procedures in driver training.

D: Day-to-Day Activities

Outline all of the security-related activities carried out on a daily operating basis. Because this subsection will describe transit procedures in detail— and because the Program and Plan are being developed using a systems approach which considers all elements of the transit system (environment, people, procedures, and property) — this section of the Plan should be of significant size. It should consist of:

1. standard operating procedures,
2. emergency operating procedures, and
3. those security related tasks that are subsystems of other transit related activities.

Standard operating procedures (SOPs) are those daily activities and tasks intended to accomplish any function within the transit system. These usually compose the rules and policies of the transit system. Only those that affect or are affected by security need be described here. However, due to the comprehensive nature of a good security program, this will include many activities. Proactive, reactive, and neutral activities will be included to whatever extent they are built into standard operating procedures.

Include all appropriate personnel in the development of standard operating procedures and consult outside sources as necessary. All SOPs impacting security should be described. The following are some activities that might be included:

- operators leaving the vehicle for breaks
- operators leaving the vehicle at the end of shifts
- securing lots and yards at the close of business
- securing buildings at the close of business
- distributing facility keys and assignment of access
- terminating employment
- collecting and counting revenue
- securing other vehicles
- securing other equipment
- patrolling of facilities
- daily activities of security staff
- response to potential security breaches
- security-related activities of station attendants, train operators, and drivers
- shift responsibilities for station attendants
- operator procedures for handling security threats

Those subtasks that have few security-specific tasks may be abridged to include only background and security-specific procedures and be described in detail elsewhere. This might apply to purchasing procedures, for example.

Emergency operating procedures (EOPs) are those special procedures for nonroutine but serious occurrences, such as responding to alarms. EOPs also include contingency plans for nonpredictable occurrences that may have critical or catastrophic consequences, such as power failures or natural disasters.

Detail the responses to actual security breaches, as well as all other emergency operating procedures that may impact security. At the very least, the following EOPs should be described:

- emergency reporting
- emergency handling by security staff
- emergency actions by front-line staff
- dispatcher responses

- system actions for
  - minor security breaches
  - crimes against passengers
  - violent crime
  - bomb scares
  - hostages
  - highjackings
  - burglaries
  - other specific security breaches
- incident investigation
- media communications
- contingency plans for
  - power failures
  - natural disasters
  - terrorism

The Plan is intended to be a living document and will need to be updated in real time. Describe each set of operating procedures on a separate page, with a revision date, so that new or revised operating procedures can be easily inserted. This will also help administrative assistants responsible for distributing Plans to managers and/or assignments to copy all of the appropriate pages for each set of staff. The format for a set of operating procedures includes:

- title
- separate page for each set of procedures
- descriptive indicating affected personnel
- level of restriction
- list of procedures
- highlighted changes (optional)

The operating procedures may be organized in any fashion that is clear to all readers. This may be alphabetical by title, by department, or by first standard then emergency operating procedures. Be sure to include any new procedures related to proactive security measures and that all new procedures have been put through an implementation process. To help

emphasize changes in policy, revisions may be highlighted. The following shows an example of a security-related standard operating procedure for driver breaks.

Leaving of Vehicles for Breaks

Revised Date

This set of procedures defines the steps required when operators leave their assigned bus to take mandatory and requested breaks, and applies to drivers, dispatchers, and schedulers ONLY.

1. Breaks must be taken at least every four (4) hours.
2. Breaks must be taken at the end of the line, or at designated layover facilities.
3. Drivers desiring a break must notify the dispatcher to formally request a "10-6" and give their location.
4. Dispatchers, after approving the location and confirming that sufficient time is available to take the break, shall provide approval or disapproval, which drivers shall abide by.
5. Passengers shall not be allowed to board the bus until the driver returns.
6. Driver shall properly park the bus, turn off the engine, take the key, and lock the doors.
7. Breaks shall be limited to 20 minutes.
8. Before boarding the bus, driver shall inspect the outside of the vehicle for tampering or damage.
9. Driver shall notify the dispatcher upon return.

Chapter 6
V: Threat and Vulnerability Identification, Assessment, and Resolution

Chapter 6
V: Threat and Vulnerability Identification, Assessment, and Resolution

Section V of the Plan will outline how security threats and potential threats (vulnerabilities) will be identified, evaluated, and resolved. Identification and data collection are crucial to this process. Many transit systems have discovered that a lack of statistical and historical data on security incidents has frustrated attempts to resolve problems. Establish a number of methods to collect and communicate security information so that real threats and vulnerabilities may be identified, examined, and appropriately resolved. Account for each of the following:

V. Threat and Vulnerability Identification, Assessment, and Resolution

A. Threat and Vulnerability Identification
    1. Security Testing and Inspections
        a. Phase I: Equipment Preparedness
        b. Phase II: Proficiency Evaluation
        c. Phase III: System Effectiveness Exercise
    2. Data Collection
    3. Reports
    4. Security Information Flow

B. Threat and Vulnerability Assessment
    1. Responsibility
    2. Data Analysis
    3. Frequency and Severity

C. Threat and Vulnerability Resolution
    1. Emergency Response
    2. Breach Investigation
    3. Research and Improvements
    4. Eliminate, Mitigate, or Accept

Provide a road map for the flow of security information. It should cover the system tests and inspections to be conducted, how information is collected from other sources, how this information should be reported to do the most good, and how the information should flow throughout the system.

A: Threat and Vulnerability Identification

Describe the methods the transit system will use to identify the threats to the system and the vulnerabilities of the system. A public transit system is very vulnerable to certain types of threats, including vandalism and graffiti on buildings and equipment, pick-pocketing and purse snatching, fare avoidance, trespassing, and many other security problems. A transit system can face many threats to its security including curious children, destructive passengers, criminals, and even disgruntled workers. A potential security problem exists when these two components — *threat and vulnerability* — coincide.

It is impossible for a transit system to be completely secure. Security is a process of risk management. It is necessary to identify the major vulnerabilities and to identify threats to which the system is subject. These identifications should be done independently so that assumptions about vulnerability do not hide the possibility of problems with threats. Once the vulnerability and threat areas are brought into focus, the security resources can be applied to solve specific problems.

1. Security Testing and Inspections

The primary purpose of security system testing and inspection is to assess the vulnerability of the transit system to a security threat. It can also be used to enhance preparedness and to promote security awareness. The testing and inspection portion of the Plan needs to promote and ensure

- equipment preparedness,
- employee proficiency, and
- system effectiveness.

This is accomplished by designing a testing program that does more than assess the current state of security. It can be used to upgrade the overall effectiveness of the staff by providing training in security techniques and by fostering teamwork between the security staff and other employees of the transit system. Employees are encouraged to identify problems and to recommend possible solutions. The system will only perpetuate security deficiencies that show up on inspection reports.

It is recommended that the following three-phase approach be used to evaluate the current state of security preparedness. Conducting the inspection in stages will improve problem identification, provide training opportunities for the security forces, and reinforce the value of security throughout the system.

Phase	How	Why
I. Preparedness	Confirm the equipment preparedness of the system. Ensure that security equipment is operable and in the location where it belongs.	People can be expected to perform well only if their equipment is available and in good repair. The inspection for equipment preparedness prior to the proficiency evaluation will eliminate problems before they can obscure the results of proficiency tests.
II. Evaluation	Assess the proficiency of employees in using the equipment provided. Ensure that employees demonstrate knowledge of both how and when to use individual equipment.	The proficiency assessment, along with the preceding inspection for equipment preparedness, will decrease security problems due to unpreparedness.
III. Exercise	Evaluate complete security systems by employing exercises. Design exercises that require coordination between different segments of the security system.	This will assess how well the system functions as a whole. It will involve all levels of the security department, from supervisors to response teams, and will assess how well the security department is integrated with the rest of the transit system.

Table 6-1. Phases of Security Preparedness Evaluation

a. Phase I: Equipment Preparedness

Describe how equipment inspections are to be conducted with the intent of minimizing vulnerability. The following items will need to be specified:

Equipment lists

These include individual, vehicle, and facility lists which describe the security equipment and its location. Lists will be used to check off the presence of security equipment.

Maintenance records

These can be in the form of log books, maintenance cards, or automated records of inspections, routine maintenance, tests, and equipment repairs. This information should be reviewed by an experienced security individual to ensure that the required equipment has been well maintained.

Equipment tests

A list should describe how a particular piece of equipment should operate and what task it will accomplish. Tests should be used to spot check security equipment to ensure proper operation.

Several levels of equipment deficiencies may be identified during the inspection. Specify in general terms what constitutes acceptable levels of equipment preparedness. For instance, if a single video camera is used to monitor a station platform, the camera must be functional. If two cameras are used, then the loss of one may be tolerated for short periods of time.

Any equipment conditions found to be unacceptable during the inspection should be corrected prior to proficiency evaluation. Once the equipment tests have been completed satisfactorily and the deficiencies corrected, the security system is certified as ready for proficiency evaluation. It should be noted that during the equipment inspection, it is in the best interest of the employee to point out existing equipment problems since they must live with uncorrected problems during the proficiency part of the inspection.

b. Phase II: Proficiency Evaluation

Describe how employee proficiency evaluations are conducted. The following items will be specified:

Security records list

This is a list of the records that security staff complete regarding routine assignments and incident reports. It should be used to ensure that responsibilities are understood and are being followed.

Performance lists

These include requirements to demonstrate proficiency with equipment operation and willbe tailored to individual positions.

Procedural lists

These will be used to check the employee's knowledge of the proper procedures to follow when confronting a security situation.

Describe what is considered a minimum acceptable level of employee skill and stress the opportunity for instruction that this part of the inspection presents. The goal of this portion of the inspection is to bring individual proficiency up to the level at which a coordinated system exercise can be successfully conducted.

c. Phase III: System Effectiveness Exercise

Describe how to conduct a security system exercise. The following items will need to be specified:

Operational assignments

This list will provide the positions and staffing levels for security staff under different situations. It will be used to identify any deficiencies in staffing or any problems with assignments.

Operational scenario

This is a practice script which will be used to guide a security exercise. It will describe what information will be provided to employees and what actions should be taken. The Plan may refer to the full script filed elsewhere, since the Plan may be widely distributed to individuals/ security functions who are to be tested.

Measures of effectiveness

For each of the following categories, develop a measure of effectiveness.

- command and control
- communications
- effectiveness of operations
- alternative strategies
- security priorities
- coordination with community
  - police
  - fire and rescue
  - media

An exercise should simulate operations in as realistic an environment as possible. The exercise should be supervised by experienced security individuals who will score the operation and prepare recommendations for improving procedures or training. Include several fully scripted operational scenarios, providing a comprehensive security system evaluation while keeping security personnel guessing as to which exercise will be conducted at any given time. This part of the inspection should be used to build teamwork among the different parts of the system and also to build confidence in their ability to handle difficult situations.

Provide guidelines for conducting these inspections and exercises. It needs to provide an annual schedule showing how often each type of test needs to be conducted. Routine equipment inspections should be done quarterly to encourage maintenance and to quickly catch security problems. Proficiency evaluations should be conducted annually to maintain security consciousness. In positions of high turnover (such as security guards) a more frequent evaluation may be needed. An ongoing program can sustain communications and coordination between the transit system and the community if local agencies are involved.

2. Data Collection

Focus on the collection of information dealing with possible security threats to elements of the transit system. Within the transit system there is a great deal of information to help a security manager allocate resources. Sources include incident and breach reports, passenger complaints, and personnel records. Identify these sources, prescribe procedures for accessing this information, and state limits on the distribution.

Beyond internal resources, the transit system needs to maintain liaisons with local police, state and federal officials, and any local organizations whose activities may affect the system. Identify sources of outside information such as local police reports and Department of Justice/Uniform Crime Reports. It should describe how to access this information and what special procedures need to be used to identify transit-related information from the large quantities of crime information available. Provide names, addresses, and phone numbers for points of contact in an appendix. The collection of information dealing with possible threats and vulnerabilities to the system compliments the preparedness testing described above.

In collecting information, it is important to keep in mind that all threats are not equal. Low threat categories generally include current employees, passengers, and organizations. High threat categories include disgruntled former employees, vandals, criminals, and terrorists. *(A terrorist may seek employment in order to gather intelligence and to gain access to critical systems.)*

Describe how certain information will be provided to security staff. For example, the security department should be notified whenever an employee who has had access to sensitive information is dismissed. Include a list of the job categories to which this applies and should describe the routing of customer complaints and/or threats. For instance, state how security staff will be notified whenever it becomes known that a potentially troublesome group (a crowd for an event, a group demonstrating) will be using the system. Notification does not mean that action will necessarily be taken. The security staff needs to be aware of potential problems so they can take steps if they deem then necessary.

Describe how information on actual occurrences will be obtained by the security department. An incident report should be developed to collect information about security incidents occurring in the system. As a minimum, each incident report should include:

- date/time
- location
- mode of transit affected
- persons involved
  - employees
  - security personnel
  - passengers
- narrative of incident

- estimated cost of damage
- disruption of service
- security action taken
- name of supervisor

The purpose of these reports is to alert the security system to threats so that actions can be taken to improve system security. Spell this out clearly. These reports should be kept simple and should not be used in the investigation of liability issues or in other forms of investigation.

A security department deals with sensitive information concerning employees, passengers, organizations, and criminal activities. Lay out procedures for safeguarding this information. Procedures should

- limit access to records,
- limit distribution of security reports, and
- distribute only general and summary information in public reports.

3. Reports

Describe the types of security reports that must be developed and how they should be distributed. Reports provide summary data concerning the security information that has been collected. Three types of reports are generally used:

1. Management reports
2. Statistical reports
3. Special requests

Periodic management reports provide upper management with the information it needs to deal with general questions concerning the system's security. These reports will summarize the number of security incidents and breaches by type (lost revenue, repairs, damage claims, and liability) and the dollar value. If needed, a list of incidents and breaches over a certain damage level measured in dollar value can be grouped together with a summary of ongoing security projects. The management summary report should be comprehensive enough to give management a clear picture of the effectiveness of system security.

Statistical reports are used by the security staff to determine areas where problems are occurring and to identify any trends in the threats to the system. Place limits on the distribution of these reports because they will contain sensitive information. Statistical reports should be placed in categories and indicate

- the numbers of incidents and breaches taking place,
- the number of perpetrators identified, and
- the cost to the system of the different types of security problems, and other associated information.

Special requests for information should be handled on a case-by-case basis. The information should be stored in a manner that facilitates access. Incident and

security breach databases, which contain a limited number of key indexed fields, will provide sufficient information to satisfy most requests. The Plan may specify who is authorized to make special requests and place limits on the dissemination of the information.

A typical activity undertaken by municipal law enforcement agencies is to plot crimes on a map and associate them with time periods. It is common for criminals to have recognizable patterns of behavior, including both location and time of day. Transit crime should be similarly plotted and tracked over time to identify any patterns.

4. Security Information Flow

Describe the methods used to collect, store, and disseminate security information throughout the system. It will also describe methods for storing the information so that it will be available when needed.

As shown in Figure 6-1, the main sources of information are incident and breach reports, inspection reports, and information from outside sources. All of this information should be sent to a central point of contact identified by the Plan. For small transit systems, this information can be kept in files and used periodically to review security performance and to produce statistical reports. However, if the system is large, a security database should be developed to store, analyze, and retrieve security information. The database can be indexed by standard system identifiers such as:

- location
- mode
- patron impact
- estimated cost
- service disruption
- security action taken

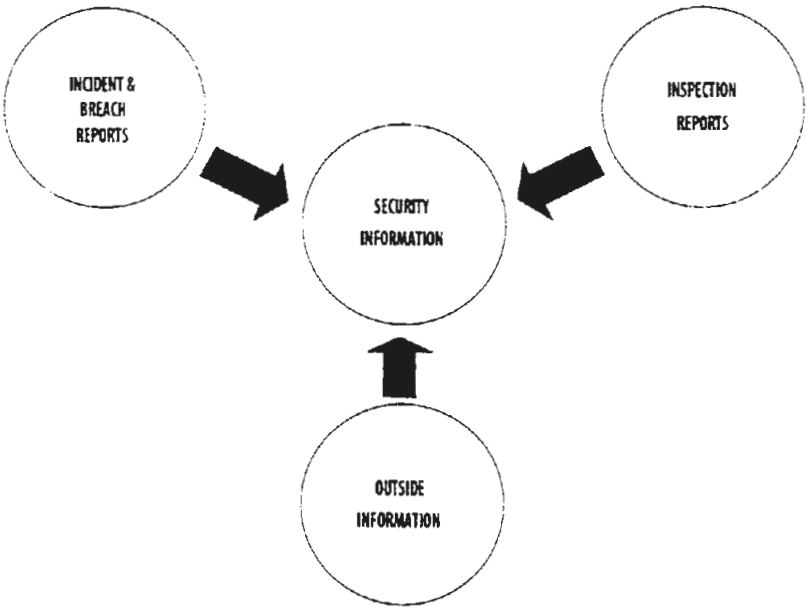


Figure 6-1. Security Information Sources

Once this information is stored in a central location, it can be used by the security system to see where problems are occurring and where improvements can be made. Describe how the different types of information should be handled before being added to the central file. A routing plan for items, such as the inspection report, should be developed and included. An example of such a routing plan, in this case for a security breach report, is shown in Figure 6-2.

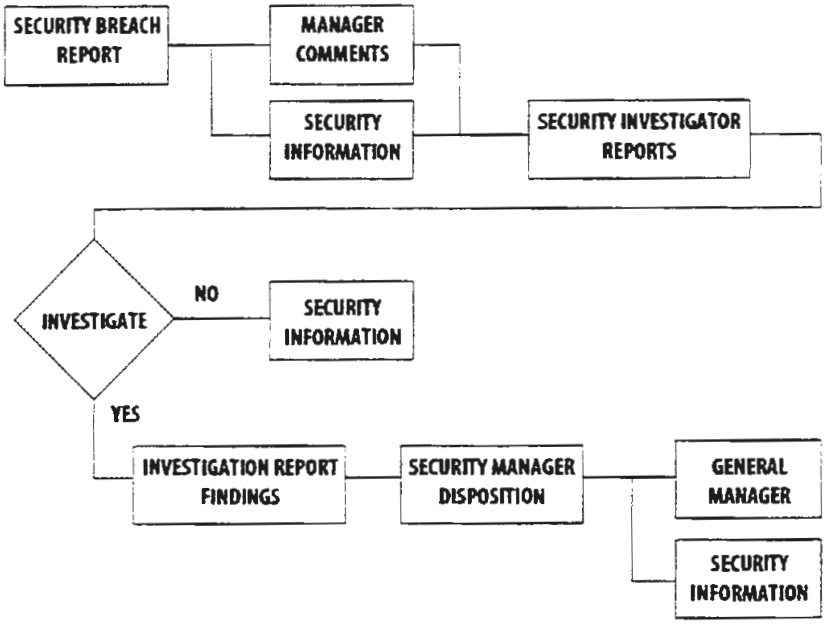


Figure 6-2.
Security Breach Report Processing

Describe who will receive the reports generated by the security information system. It should consider the sensitivity of the information, its usefulness to the person receiving it, and alternative ways of making the information available. A distribution list such, as shown in Figure 6-3, will be sufficient to illustrate to whom security reports will be sent. When this section is completed, the reader should have a clear understanding of the sources for security information, how it is handled during the collection phase, how it is stored, and to whom it is distributed.

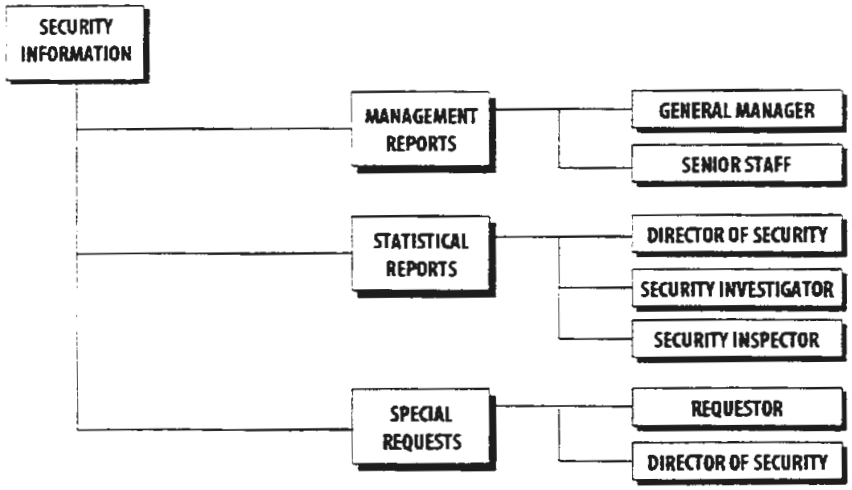


Figure 6-3.
Security Information Distribution

B: Threat and Vulnerability Assessment

Describe how the security information will be analyzed to determine where the system is vulnerable and what threats are most likely to be experienced. It should assign responsibility for security assessment, describe how the information will be analyzed and what will be done with the results.

1. Responsibility

Spell out who is responsible for threat assessment. Since the results of the assessment will direct the deployment of security assets and determine which areas of the system will be protected, the individuals assigned to conduct the threat and vulnerability assessments are critical to the success of the Program. Describe minimum qualifications of the analysts and supervisors, and the qualifications should include:

- security experience
- knowledge of the system
- familiarity with the community
- knowledge of statistical methods and their limitations

If the transit system is large enough, the persons assigned should be rotated back to direct security work periodically. This will keep their experience level high and current. In addition, security analysis can be enhanced by using employees from all departments. This will provide a clearer picture of how vulnerable the system is perceived to be. The experienced judgment of the security committees can serve to validate individual assumptions.

2. Data Analysis

Describe how the information will be analyzed to assess the current level of security in the system. Vulnerability and threat are the two major factors involved in this analysis.

- Vulnerability is the susceptibility of the system to a particular type of security hazard. Vulnerabilities can be corrected, such as putting guards on trains or doing background checks on money handlers.
- Threats are specific activities that will damage the system, its facilities, or its passengers. For example, threats include the potential for personal assault and vandalism.

Vulnerability/threat analysis can be performed. First, list all of the facilities and systems that make up the transit property. Second, list all of the possible threats. Figure 6-4 illustrates a partial listing of a vulnerability analysis. Lists need to be derived from the information in the security system database. For example, all of the sites for inspections should be listed in the facilities and systems list. Similarly,

all of the threats identified in incident reports or from police sources should be listed.

For each facility or system on the list, an assessment should be made concerning how susceptible it is to each threat. Where a facility or system intersects with a threat, a ranking should be determined indicating the vulnerability of the system to that particular form of threat. The control center, for example, might be determined to have a very low potential for vandalism and be assigned a rating of 1 on a scale of 0-4 (although any scale may be used). In contrast, buses are highly vulnerable to vandalism and might be assigned a rating of 4. When the matrix is completed, it will reveal where security problems are most likely to occur.

	THREATS		
FACILITIES & SYSTEMS	VANDALISM	ROBBERY	SERVICE DISRUPTION
FACILITIES			
CONTROL CENTER			
RECEIPT ROOM			
SYSTEMS			
CONTROLS			
POWER DISTRIBUTION			
SUBWAY			
BUSES			

Figure 6-4. Example of Vulnerability Analysis

3. Frequency and Severity

Once vulnerability has been assessed, there is a need to predict which threats are most likely to occur. Direct that this part of the analysis be conducted separately from the vulnerability analysis. If it is done in conjunction with the vulnerability analysis, the evaluators may focus only on perceived threats and not on the broader vulnerability issues.

The threat analysis should rank each of the vulnerability categories based on the likelihood that the threat will occur. When a high threat coincides with a high vulnerability, security should be focused on that area. The severity of the results of a security breach also plays an important role in decision making. The painting of graffiti on a bus is unsightly and should be prevented; however, it does not prevent the bus from generating daily revenue. In contrast, a bomb explosion in a parking garage at an underground railroad facility and station could cause deaths and significant injuries and significantly reduce or prevent normal revenue service. Threats and vulnerabilities with high levels of severity and frequency should be given priority.

C: Threat and Vulnerability Resolution

Describe how identified threats will be addressed by the transit system. Some threats may demand emergency response; others may require a long-term

project; and still others may just be accepted as part of business with no action taken. Discuss some of the factors that go into making such decisions and some of the criteria used (e.g., frequency and severity) to draw conclusions.

1. Emergency Response

Identify what security criteria need to be met in order to activate certain types of emergency response. For instance, it could be assumed that sometime in the future there will be a demonstration by a group known to be destructive. As a result, emergency deployment of additional security personnel may be necessary. Similarly, it could be assumed that a chain of breaches will threaten to disrupt the transit system, and it may be necessary to add security personnel to buses and trains to increase their visibility. Also, if there is a direct threat against the transit system that could involve passenger safety, some portion of the system may have to be shut down and passengers diverted. These types of threats and others particular to the individual system should be anticipated, explained, and a policy set for the appropriate type of response.

Describe the mechanism for activating certain types of emergency response, including who is authorized to initiate an emergency response, what levels of response are possible, and for how long emergency responses can be maintained.

2. Breach Investigation

Describe how incidents will be investigated to determine the best approach to lowering the risk. The goal of a breach investigation is to determine what circumstances led to the breach. In an accident investigation, this is referred to as finding the probable cause. The following subjects should be addressed in the breach investigation and resulting report:

- description of the breach
- identification of the source of the threat
- physical description of the location
- description of equipment involved and its physical condition
- human factors including
    - conditions at the time of the breach
    - training and knowledge of procedures
    - performance during the breach
    - conditions resulting from the breach (e.g., injuries)
- environmental conditions
- actions taken to mitigate the breach

- command and control effectiveness
- determination of probable cause
- recommendations

Information on these subjects should be collected in an investigative report and submitted to management for action. In extraordinary cases, this effort may have to be coordinated with the activities of state and federal investigations, and possibly with investigations by the National Transportation Safety Board.

3. Research and Improvements

There will be some cases when the security analysis reveals a problem that does require additional study to determine how the risk can be managed. Provide criteria for long-term improvements in identified security-risk areas. It is not expected that most transit systems will be able to afford the development of their own security technology, but there are often occasions when new technology offers security improvements that a progressive system can adopt to its advantage.

An example would be a need to have better control over access to particular areas. Typically, this is done through key/lock systems having individual and master keys. These systems become more vulnerable over time and the need to change locks frequently can prove costly. A transit system may want to try a card-key system which provides access through the use of an electronic code on a plastic card. This would allow the locks to be reprogrammed frequently, and the system would not be compromised through the loss or theft of even a master card.

Describe pilot programs where new technology can be installed and evaluated. Criteria should be established for acceptance of a new system. It should be able to prove itself in terms of (1) effectiveness in an area of vulnerability, (2) cost with a rapid pay-back period, and (3) life-cycle dependability by not requiring long-term maintenance. The demonstration period should be used to verify all of the claims for the new system before a full-scale commitment is made.

Describe circumstances where cooperation with other transit systems in assessing new technology should be explored. There are very good opportunities to share innovation among transit systems because what works for one will often work for others.

Provide a means for employees to recommend improvements to the system. This has been shown to be one of the most cost-effective and productive sources of new ideas for system security. Consideration of employees' proposals will instill greater commitment. Provide procedures for submitting suggestions, a review process, a feedback system to let individuals know that their suggestions are being considered, and reward system for suggestions that are adopted.

4. Eliminate, Mitigate, or Accept

Make it clear that there are three possible alternatives associated with security problems: eliminate, mitigate, and accept.

Eliminate

Eliminate the problem. This may be done through redesign, retraining, or changing procedures.

Mitigate

The usual choice is to mitigate the threat by increasing surveillance, changing procedures, or bolstering the presence of security forces. Although this is a risk-management problem that the Plan must discuss, in reality, the Plan cannot present more than general guidelines on risk management.

Accept

There will be cases where the risk will just have to be accepted. Either the threat is so remote that it is not likely, or its impact on the system may not be sufficiently dangerous to warrant any action. The factors that go into the decision as to what level of risk will be tolerated have to do with the environment in which the system operates and the resources available.

Chapter 7
VI: Implementation and Evaluation of System Security Program Plan

Chapter 7
VI: Implementation And Evaluation of System Security Program Plan

Section VI of the Plan will be concerned with providing details on how it will be implemented and how progress will be evaluated. This stage is crucial to establishing an effective Program. If the Plan is incomplete, flawed, or not supported by the appropriate staff, the security-planning efforts may be futile. Having completed the Program Plan, security managers will need to ensure that the program is effective in eliminating, mitigating, and handling security threats and breaches.

The first time a plan is developed and implemented, the planning process will take longer than it will once the framework has been established and proactive security measures are being developed regularly by the Proactive Security Committee. Remember the following when developing the first Plan:

- goal, objectives, and tasks must be established
- approval must be obtained
- security information must be gathered
- solutions must be researched, and
- text must be committed to paper.

In modifying and implementing a program that is already in place, most of the Plan will already have been written. If the program in place is effective, most of the changes and solutions will have been already worked out. The procedures for implementing the Plan should be included in the Plan itself. Implementation will require development of the following:

VI. Implementation and Evaluation of System Security Program Plan

A. Implementation Goals and Objectives

B. Implementation Schedule

C. Evaluation

1. Internal Review — Management
2. External Audits

A: Implementation Goals and Objectives

In addition to the goal and objectives established for the program itself, major goals and specific objectives should be established for implementing the Plan. These goals and objectives will reflect the Plan document as a part of the Program. The goals of implementing the Plan are different from the goals of the Program. The Plan should ensure that the

- transit staff understands exactly how the Program affects them,
- program receives appropriate support from management,
- activities described in the Plan are undertaken, and
- tools necessary for carrying out the Plan are provided.

The primary goals of implementing the Plan will be to:

Establish a Program.

After the Program is established, this primary goal will change.

Define and Modify the Program.

A number of other goals will support this primary goal. The transit system should adopt and record the implementation goals most appropriate to itself.

Describe the Program Clearly.

Because the intent of the Plan is to clearly establish an effective Program, the Plan should accurately describe the transit system, the context of the Program, and the security activities. The final stages of the Plan development and initial stages of Plan implementation should include a review of the Plan for content. The Plan should reflect the current activities and procedures of the transit system. In addition, professionals (other than the authors of the Plan), should evaluate and critique the Program immediately prior to implementation. Supporting objectives may be to

- ensure that the Plan is comprehensive and complete,
- ensure that all managers and supervisors understand the objectives of the program,
- ensure that the Plan is current, and
- evaluate the Plan.

Communicate the Program to All Affected Persons.

Supporting objectives would be to

- obtain concurrence from the Board of Directors,

- distribute the Plan to all managers and supervisors,
- require managers and supervisors to communicate the Plan to staff, and
- resolve all questions related to the Plan and Program.

An endorsement of the Plan must be obtained. By submitting the Plan to the Board of Directors for approval, the transit system will ensure that the document will provide for its security and for the security of its patrons. A "hands-off" Board may approve only the concept of the Program, yet this support will help drive the implementation of the Plan by emphasizing its importance to the transit system and to the community. The Board may also read the detailed Plan and offer some criticism. It can be expected that some changes may be required, and revisions should be scheduled into the early stages of implementation. This critique will capture the support of the transit system's governing body for security-related activities. This support can be especially valuable in the case of a security breach that attracts the attention of the community or for any fiscal requirements related to implementing proactive security measures.

The Plan should be distributed to upper-level managers and supervisors before the rest of the transit staff. Those staff members supervising others must be completely familiar with the Program before full implementation is initiated. This will enable the lead security personnel to deal with questions and work out details with the supervising staff who will be truly responsible for seeing the program through. The supervising staff will then be able to effectively communicate Plan contents (the Program) to all other personnel.

It is unlikely that the transit system will want to distribute copies of the entire Plan to every employee. If the Plan contains all of the detail necessary to prevent and counter security breaches, it should not be shared with the public. For example, standard operating procedures for fare revenue collecting and counting should be established during the planning process but should not be distributed to every employee. Abridged Plans may be distributed to most staff, containing

- introductory material,
- goal and objectives of the Program,
- transit system description (optional),
- management of the Program (especially division of security responsibilities),
- planning roles and responsibilities (optional), and
- appropriate day-to-day tasks, roles, standard operating procedures, and emergency operating procedures.

Any transit system employee may have questions about the new Plan or his or her own role, so it is essential that questions be answered by supervisors. Although the goal has been to make the Plan self-explanatory, people will have questions about its impact on daily system operations and on their own functions within the system. Any new ideas that arise from the implementation process that should be considered for modified plans should be recorded in a file .

Put in Place the Means to Accomplish Security Tasks and Activities Established by the Plan.

Supporting objectives would be to

- ensure that all affected staff members are aware of any new responsibilities, new operating procedures, and changes to the Program,
- provide necessary training,
- establish the Proactive Security Committee (if new),
- establish the Security Breach Review Committee (if new), and
- obtain and install required equipment.

The most important part of implementing the Plan is to ensure that there is a facility to accomplish assigned responsibilities. Having personnel understand the specific changes that affect them is key to this process. Supervisory staff will have to clearly explain these changes and, in some cases, provide staff with the necessary skills to perform new tasks by means of training. Training may range from coaching people about filling out new forms to scheduling groups of operators for a new course. All major training requirements should be identified and described in full under the Roles and Responsibilities section of the Plan in the "Training" description.

During Plan implementation, the Proactive Security and Security Breach Review Committees should be established. If the committees are already established, the membership and organization may be changed. For example, driver representatives might serve for one year on a security committee. At this time a new operator might be selected. Ordinarily, the full membership of the committees does not change very often. Identify and state the objective of establishing or modifying the committees, followed by a time line for the specific tasks required to do so. The Proactive Security and Security Breach Review Committees should be discussed in detail in the section entitled "Management of System Security Program Plan."

In establishing the means to accomplish security tasks and activities, one objective must be to obtain and install required equipment. This task may range from photocopying new forms to outfitting a new transit security or police force. The process should be undertaken as soon as possible following the initial implementation. Lead time required for procurement can be extremely long due to the need for fiscal approval, bid processes, back orders, assembly, shipping, installation, and adjustments. Any delays in procurement will delay the realization of security objectives. New equipment might include the following:

- incident reports
- locks and keys
- radios
- call boxes

- ❍ flood lamp bulbs
- ❍ weapons
- ❍ alarms
- ❍ mirrors
- ❍ revised schedule fliers
- ❍ closed circuit TV cameras and monitors

Provide a Means to Accomplish Security Tasks.

This is especially important while implementing new proactive measures. Extensive new activities within the Program (such as undercover operations) should be identified as implementation objectives in their own right.

Execute Specific New Security Subprograms.

The objectives should be specific, each stating the new subprogram, such as "continuously monitor all stations." Specific tasks should be associated with each of these objectives, and milestones with dates should be included.

B: Implementation Schedule

To carry out the implementation of the Plan, a time line or schedule with specific milestones should be developed. The schedule should be based on the implementation goals and objectives and on the overall Program goal and objectives that relate to the implementation of new subprograms. The schedule should proceed chronologically from the completion of the Plan document to the beginning of the yearly plan modification process. This schedule should include specific dates for each task required for implementation.

A typical schedule for the implementation of a new Plan is shown in Table 7-1. This schedule considers a new plan being written by an active top manager with other ongoing responsibilities. The actual schedule may be longer or shorter depending on the size of the system and the demands on the contributors to the Plan. However, shorter implementation schedules are preferred. The transit system's schedule should also include actual dates. The sample schedule does not include the specific tasks associated with implementing a new subprogram. These specific tasks will vary depending on the Plan.

ACTIVITY	DAY
Write Security Plan	Days 1-30
Read Transit System Security Program Planning Guide	Days 1-3
Obtain Approval to Develop Security Program	Day 4
Collect Information on Current Activities	Days 5-7
Identify and Assess Security Threats and Vulnerabilities	Days 8-10
Consult with Management Staff	Days 8-30
Consult other Security Documents	Days 8-30
Consult with Other Transit Systems by Phone	Days 8-30
Develop Proactive Security Measures	Days 10-18
Finish Draft	Day 20
Have Plan Reviewed by Other Managers	Days 20-23
Edit Security Plan	Days 22-30
Finalize Security Plan	Day 30
Submit Plan to Board for Approval	Day 31
Revise as Necessary	Day 35
Communicate the Security Program to All Personnel	Days 36-45
Distribute "System Security" Memo to all Transit Personnel and Other Interested Personnel Endorsing the Security Plan	Day 36
Distribute Security Plan to Management Staff	Day 36
Meet with Managers	Day 38
Managers Distribute Abridged Plan, Procedures, and Assignments to All Personnel	Days 39-45
Share Security Plan with Local Chief of Police	Day 40
Establish Means to Accomplish Security Tasks and Activities	Days 39-69
Managers and Supervisors Ensure that All Subordinate Staff Understand Roles and Responsibilities, as well as Applicable Standard and Emergency Operating Procedures	Days 40-53, and ongoing
Establish Proactive Security Committee	Day 45
Establish Security Breach Review Committee	Day 45
Obtain and Install Required Equipment	Days 39-69
Implement Specific New Subprograms	Days 39-69
Specific tasks for specific subprograms	Days 36,37,38
Conduct Ongoing Operations With Maximum Security According to System Security Program Plan	Ongoing
Evaluate Security Plan Implementation and the Security Program	Ongoing
Internal Review by Management Staff	Days 36-69 and Ongoing
Obtain External Audit	Days 120-165
Modify Security Program and Plan	As necessary
Schedule Security Plan Update	Day 200

Table 7-1
Example Schedule for Implementing a Security Program

C. Evaluation

It will be necessary to evaluate constantly the program during implementation. This evaluation process should extend from the initial draft of the Plan through full implementation. The evaluation must reflect the fact that system security is based on a comprehensive planning process for a program that extends throughout the entire system. Consequently, the Plan should benefit from the review and input of internal management staff as well as external audits.

During the drafting period, reviews will enhance the quality of the Plan. During

implementation, the reviews will identify issues to be resolved as the program goes into effect and will provide feedback on the progress of implementation. Those areas responding slowly can receive the benefits of management attention and guidance. Evaluation at the time the program is expected to be fully implemented will identify those areas needing additional attention and will offer suggestions for improvement, either to fine-tune the Program or to implement new objectives in a revised Plan. Briefly explain how implementation will be evaluated. Two possible approaches can include Internal Review Management and External Audits.

1. Internal Review—Management

Following the development of a Draft Program Plan, in which security staff will have participated with assistance from other departments, managers throughout the system should evaluate the whole Plan for clarity and the specific Program it implements for comprehensiveness. Any problems with the Plan or Program identified by other managers that would hamper the accomplishment of security objectives should be worked out with the appropriate departments, and the Plan should be revised. Suggestions for changes in priorities should be submitted for future consideration and may be put on hold in favor of fine tuning the established program and proceeding with implementation.

During the implementation stage when roles and responsibilities are assigned and new programs are initiated, managers must provide constant feedback to the lead security staff. Although the supervisory staff will be busy communicating new tasks and training as necessary, managers should try to step back and assess the effectiveness of implementation. Lead security staff may want to establish weekly meetings during the initial implementation of a new Program to make use of this feedback and to smooth the implementation process.

Each member of the security department should constantly evaluate the effectiveness of Plan implementation. In part, this will be accomplished by the collection and analysis of security data as described under Chapter 6. During implementation, this evaluation should result in direct feedback to those responsible for the overall Program; that is, the General Manager and the lead security officer. Evaluation should also take the form of frequent communications with supervisors whose staff are charged with new responsibilities. Any major problem areas also should be communicated to lead security staff. Problems identified during implementation may reflect difficulties in implementation. In any case, lead security staff will be best able to provide the tools or guidance necessary to correct problems specific to implementation. Problems with the Plan or unidentified (missed) security problems are more serious and should also be handled or delegated by lead security staff.

In addition to the evaluations of managers and the security staff, members of the Proactive Security Committee and the Security Breach Review Committee should evaluate the Plan and its implementation schedule as part of their agendas. Their review of the draft Plan will ensure that the priorities recently identified will be appropriately addressed. Their review of implementation success will contribute to the enhanced effectiveness of the Plan in future years.

2. External Audits

In addition to internal reviews, regulatory agencies and peer group analyses may be used to evaluate success. These types of reviews should take place following the implementation of the program but before the Plan modification process has begun. This will enable the external reviewers to evaluate the Program in terms of its success during a normal state rather than in one of change. It also will allow lead security staff sufficient time to evaluate feedback and to prepare an effective modified Plan.

Identify those techniques that will be used to formally evaluate the transit system's Program from outside the system. It should include a schedule for requesting external audits, for contacting the executing organization, for assisting evaluators, and for discussing results.

External audits may be accomplished by the following:

Regulatory Agencies	Evaluation of the procedures for implementing the Plan may be conducted twice a year by regulatory agencies concerned with security. While the assessment of more detailed security activities of the transit system may be beyond the function of some government entities, reviewing implementation (along with objectives) may be of particular interest to funding agencies. Transit systems rely heavily on government sources for funding, and it is likely that local, state, and federal adminis trative agencies will want to ascertain that monies for transit programs are being well spent and are protected. Furthermore, the endorsement of the Program by regulatory agencies may help to reduce liability in the event of a serious security breach.
Insurance Companies	Many insurance companies provide risk management reviews and audits as part of their premium charges. Systems that do not self-insure may want to ask their insurance companies to review the Plan and Program.
Law Enforcement Agencies	Local law enforcement agencies often offer gratis security reviews of facilities and may be persuaded to review at least parts of the Plan.
Peer Group or Consultant	The transit system should compare itself and its Programs with similar systems. This can be done informally by cooperating with other systems or through more formaL reviews accomplished by a consultant. Either will inject the perspective of an experienced outsider into the evaluation process. The transit system may solicit a critique from a lead security officer from another system or a transportation planning and operations professional from a private consulting firm. Outside evaluations by such sources usually yield extremely useful feedback. The results of the review process should be incorporated into normal planning activities.

The following, Figure 7-1, summarizes the suggested internal and external evaluation process.

Figure 7-1. Example Internal and External Reviews

Chapter 8
VII: Modification of the System Security Plan

Chapter 8
VII: Modification of the System Security Plan

Section VII of the Plan is concerned with modifications. The transit system needs to specify the exact methodology that will be used for modifying the Plan to reflect changes in the operating or political environment of the system itself. As discussed earlier in this document, the Plan is intended to be a living document which is used on a daily basis. The day after the Plan has been completed and implementation activities have been initiated, it should be considered for modifications.

The modification of the plan should conform to the following outline:

A: Initiation

B: Review Process

C: Implement modifications

For example, over time it may be found that additional security is required; additional program activities need to be put into place; additional security devices, instrumentation, and procedures need to be acquired and put into place; or that a host of other activities are required. In addition, it may be found that some of the methods and procedures specified in the Plan prove to be inappropriate or ineffective and need to be remedied. Other potential revisions could be necessitated by the identification of new procedures discussed at conferences or in publications or by the generation of new forms which are more appropriate for capturing and evaluating data. Still other examples may include security problems or breaches that had previously never occurred within the transit system.

It is clear that these influences and others could develop throughout the scheduled life of the current Plan. Security officers can use post-it labels, paper-clipped notes, sample forms, and other materials to indicate updates. When the yearly revision of the Plan occurs, there should not be a need for the lead security officer to go back and recreate history in order to update the Plan.

A: Initiation

It will be necessary to state the concept for modifications in addition to the day-to-day process for their implementation. For example, the Plan may state that the Program Plan will be distributed to the General Manager, all division heads, and every member of the security department; and that abridged copies will be made available to drivers, mechanics, and administrative staff on request. Distributed copies could contain a memo, such as the one that follows, requesting that the reader/ user provide comments on any part of the Plan that they believe is inadequate or inappropriate.

MEMORANDUM

TO:

FROM:

DATE:

We have developed this Security Plan using the best information available to us at the time. We recognize that as the user and the person out on the front line, you may have good ideas about how to improve it.

Please tell us honestly what we should consider changing, adding, or deleting. Your input is vital to the maximization of security within the System.

Thank you.

Indeed, distributed Plans may each include a form for suggesting revisions or for identifying issues to be addressed, such as the one that follows.

SUGGESTION FORM
HOW TO IMPROVE SYSTEM SECURITY

Date:

I have been using the System Security Plan and have developed some ideas on how to improve it and its implementation. My ideas are as follows: _____

_____

_____

_____

_____

_____

My name is _____ and my function is_____ .
I can be reached at _____ .

A copy of the memo and/or form could be included as an exhibit or in one of the appendixes. Moreover, the Plan could state here that the lead security officer and his/her staff will maintain a tickler file so that all information is available in one location and integrated when revisions to the Plan are required. In this subsection, the Plan should also identify the procedure to be used when a modification to the program needs to be implemented immediately in order to remedy or mitigate an identified problem.

B: Review Process

The actual process used by the security department and those individuals responsible for reviewing and modifying the Program Plan needs to be discussed in this section. For example, the Proactive Security Committee could be tasked with reviewing the Plan quarterly and comparing it with actual operational experience to identify necessary changes. Another approach might be to establish a very small committee of individuals (nine months after approval of the existing Plan) who would be charged with modifying the Plan or identifying necessary changes. In either case, the committee should most likely report directly to the lead security officer. Mechanisms for including changes suggested by other department heads and/or the General Manager should also be delineated. In addition, law enforcement officials may have very positive comments which identify necessary changes. This section does not need to be long. It needs to state

- the review process,
- how it is staffed,
- what it is expected to accomplish, and
- an appropriate time line.

C: Implement Modifications

Modifications to the Plan can be manifested in several different ways, as shown in Figure 8-1. For example, a new procedure, new staff responsibilities, or utilization of new forms may be considered by the lead security officer to be of substantial enough value to require immediate implementation. In such instances, appropriate pages of the Plan should be revised, approved, and disseminated to all recipients of the Program Plan. If more training is required to implement the recommendations, the training program, the dates of training, the individuals to be trained, and other appropriate information needs to be spelled out. The process for accomplishing this requirement should be committed to paper.

Modifications that can be implemented without extensive training can be instituted on an ongoing basis under the direction of the lead security officer. These modifications can then be included in the yearly update. If this is the system's approach, it should be stated here. These are simply some suggestions as to the kinds of approaches the system may take in generating this subsection of the Plan.

It may be useful to include a figure showing the modification process to be addressed in this section. An example for discussion purposes is illustrated in Figure 8-2.

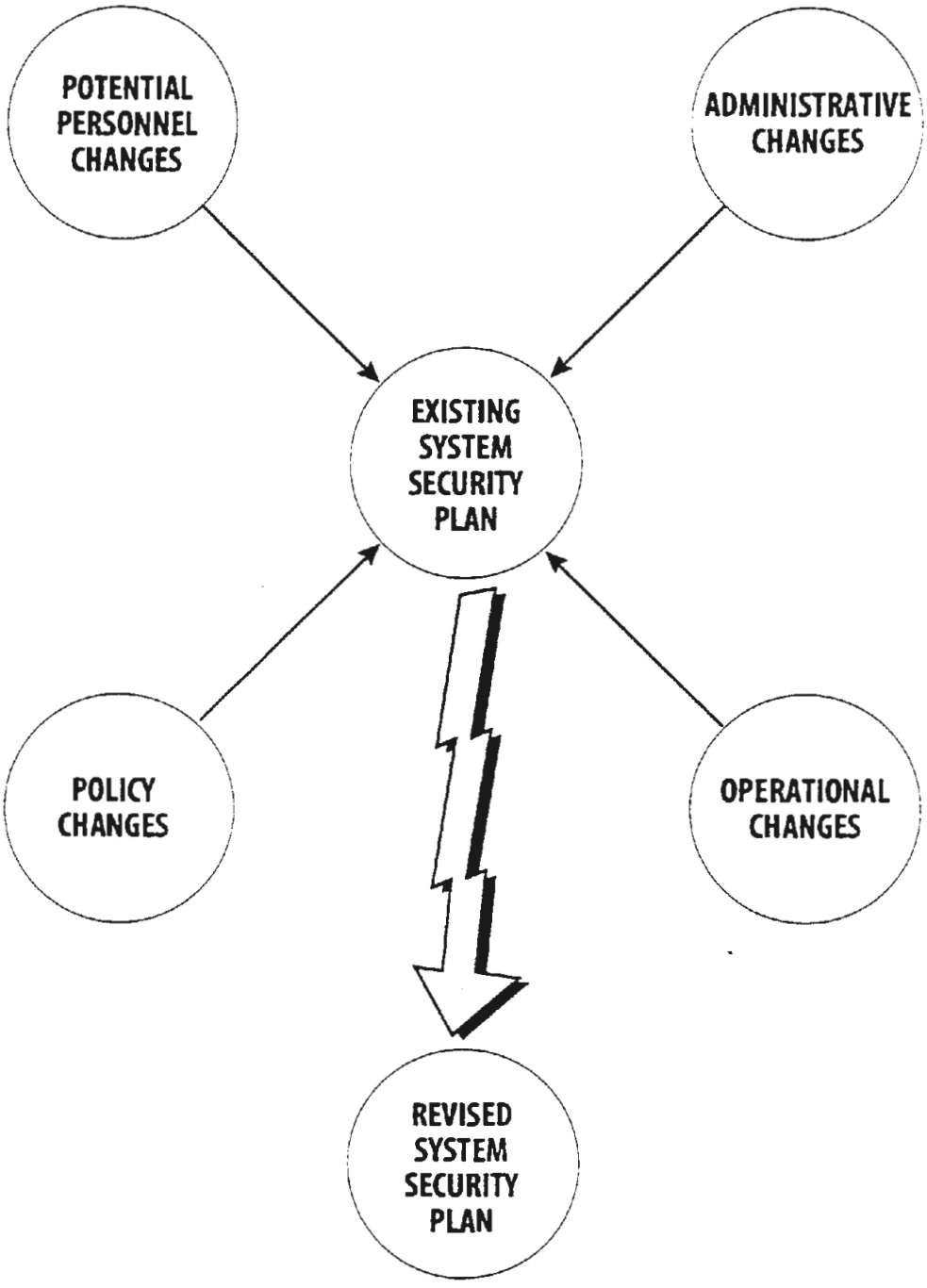


Figure 8-1.
Potential Sources of Modifications to Plan

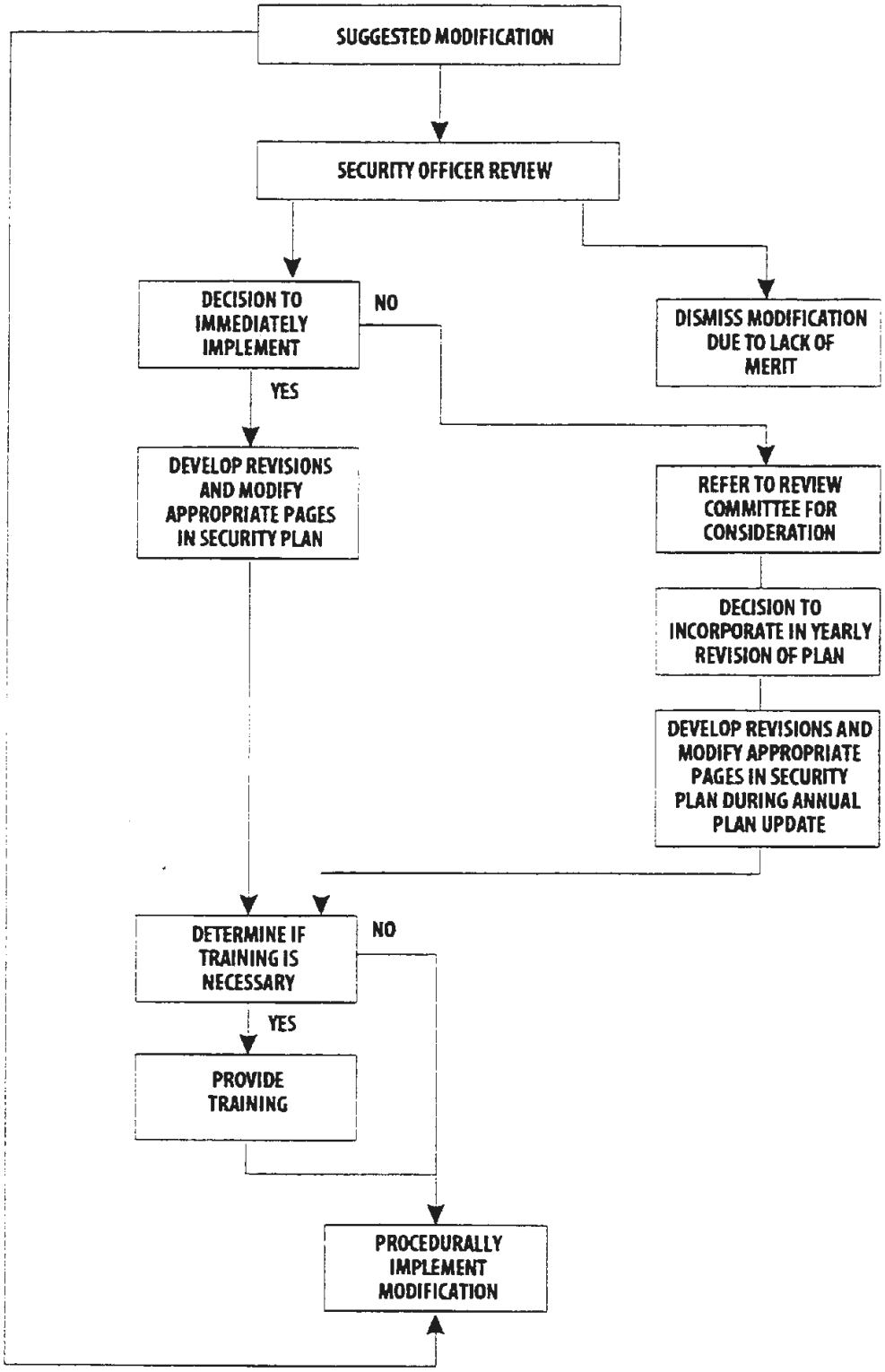


Figure 8-2. Suggested Modification Process

Appendixes

Appendix A: Bibliography

There are many good publications related to transit security. Many of these publications are outlined in the bibliography, which appears earlier in this Guide. The bibliography can be alphabetically organized in one appendix or can be organized in a variety of different sections within an appendix to reflect local interests. The bibliography of security publications has been specifically chosen to represent a very strong basic set of materials. It is not necessary for the system to have copies of all of these documents at this point in time, but it is important that the system be aware that they exist so that any additional information can be located rapidly.

If resources are available, the system may choose to automate the bibliographic citations (alone or together with their abstracts) so that key word searches can be accomplished when looking for specific information on security topics. The bibliography within the Plan will demonstrate to all readers that a significant amount of research was accomplished in order to prepare the Plan and that the concepts in the Plan are in accord with industry standards.

> ***Note: Please refer to the Biblilgraphy in the first part of this Guide. It shows you how a bibliography should be prepared and offers a list of suggested readings that will help you prepare your Plan.***

Appendix B: Glossary of Security Terms

A number of different people can be expected to read the Plan. Some will be accustomed to security topics and jargon; others may have limited or no knowledge of security. A glossary of security terms will provide readers with the information necessary to appreciate the Plan's content. The Plan can be constructed to include the entire list of relevant security terms in Section I without an appendix. Or it can be constructed with only the most important security terms defined in Section I and all remaining security terms, whether or not they are actually used in the Plan, included in an appendix.

> ***Note: Please refer to the Glossary in the first part of this Guide. It shows you how a glossary can be prepared and offers a list of terms that will help you prepare your Plan.***

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

Participation

The transit system may be involved with the law enforcement community and other agencies concerned with security. This appendix should define any and all security-related organizations to which the system belongs, in addition to those in which specific system personnel have membership and/or participate. Since system security and system safety go hand in hand and are often administered by the same individuals or group within the system, relevant involvement with safety boards, panels, committees, and task forces should be included.

For example, the Transportation Research Board maintains standing committees of transit professionals concerned with security. The city or other geographical location which the system serves may host national or regional organizations concerned with security which should be mentioned. It is important that the system make sure that it is interacting with other locations so that sharing of knowledge and innovation are possible.

Resources

In addition to the groups and organizations with which the system has formal involvement, there will be a number of organizations which are potential resources. As the Plan's Bibliography listed, this section should list those resources that are person-based. Any of the following might be included:

- American Public Transit Association (Fare Collection & Police/ Security Workshop)
- Community organizations
- Community Transportation Association of America
- Government Printing Office
- International Association of Chiefs of Police, Inc.
- Lead security officers at other transit systems
- Local police departments
- National Transportation Safety Board
- National Graffiti Information Network
- Sources of local statistical information on crime and population
- Transportation Research Board (Task Force on Transit Safety and other committees and subcommittees)
- Transportation Safety Institute

Appendix D: Security Forms and Logs

When the initial Plan is created, the system may already be using a large number of security forms and logs in day-to-day operations. They should be acquired, catalogued, labeled, and included in this appendix. If such forms do not exist, forms from other systems may be included here as examples of what is being considered for use by the system.

Additional Appendixes

Since the Plan is being tailored to meet the requirements of the local system, a great deal of freedom exists with respect to any other additional appendixes that may be needed or useful. The Plan is intended to be a living document — one which is used daily by all security professionals — so comprehensive information in these appendixes will contribute to their use. If the amount of information in the appendixes is excessive compared to the rest of the document, you may choose to bind the appendixes separately from the Plan and distribute them more selectively.