Guidelines for Development of Passenger, Vehicle, and Facility System Security Program Plans

JOHN N. BALOG, R. BENJAMIN GRIBBON, LARRINE WATSON, WILLIAM HATHAWAY, ANNE N. SCHWARZ, AND BERNARD C. DOYLE

FTA'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, revenues, 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 plan. The plan should be a complete guide for establishing and maintaining a comprehensive security program for the transit authority and the entire system for which it is responsible: including people, property, procedures, and the environment. A document designed to help transit systems outline and author the sections of a plan to implement an effective security program is summarized. Also summarized is each aspect of a security plan to ensure that when complete, the plan will (a) demonstrate management's commitment to and policy on security; (b) introduce the concept of a system security program; (c) describe the transit system; (d) establish the management of the plan; (e) detail the security program by assigning responsibilities, (e) explain how threats and vulnerabilities will be identified, assessed, and resolved; (f) describe how the plan itself will be implemented to establish or revise the program; and (g) describe how the plan will be evaluated and modified.

To achieve the highest practical level of safety and security in all modes of transit, FTA encourages all transit systems to develop and implement a transit system security plan and program that covers passengers, vehicles, and facilities. To assist transit properties in developing their security plans and programs, FTA contracted with the KETRON Division of the Bionetics Corporation to prepare a guidelines document. This paper summarizes the larger guidelines document and covers each section of an effective plan.

It is important to read the guidelines thoroughly before starting. Lead security personnel may also consult with other transit security professionals; such interaction among transit and security professionals greatly benefits the industry. Next, collect all of the appropriate security-related information within the authority. Third, write each of the specific sections outlined in Figure 1. The outline is designed for both large-scale transit properties and small rural paratransit organizations and may be adjusted slightly as appropriate to each transit system.

J. N. Balog, R. B. Gribbon, A. N. Schwarz, Transportation Planning and Operations, KETRON Division, Bionetics Corporation, 350 Technology Drive, Malvern, Pa. 19355. L. Watson, W. Hathaway, Volpe National Transportation Systems Center, 55 Broadway, Kendall Square, Cambridge, Mass. 02142. B. C. Doyle, AERA, Inc., 2011 Crystal Drive, Suite 210, Arlington, Va. 22202.

OPENING PAGES TO SYSTEM SECURITY PLAN

The opening pages to the security plan should include acknowledgments, a foreword, and a management policy statement. A wise author will credit all who contributed to the security plan or program. This acknowledgments section should also show an established and working relationship with key local entities. The foreword, which follows, should provide a clear understanding of how the plan is expected to serve as the dynamic structure for implementing an effective system security program, with a succinct expression of the reason that the plan was created.

Without a management commitment and directive or policy statement, the program and plan are almost certain to falter. The system's leader must establish a full commitment to security in the opening pages of the plan. The statement also directs responsibility for security to an individual or group and indicates full support for them and should indicate that the plan is the basis from which security roles and procedures will be implemented on a daily basis.

INTRODUCTION TO SYSTEM SECURITY

The first section of the plan, the introduction, should introduce the concept of system security and present the following key concepts according to the outline shown in Figure 1.

Purpose

A system security plan is of limited value unless it fully defines and implements a system security program. Otherwise, the plan document could simply end up on a shelf, unread and collecting dust.

Current thinking emphasizes identifying potential threats and areas of vulnerability and developing proactive, prevention-oriented approaches that will minimize them. There will, nonetheless, be security breaches; they require reactive law enforcement actions to be defined. This threat and vulnerability management, as applied to all aspects of the people,

ACKNOWLEDGMENTS

FOREWORD

MANAGEMENT COMMITMENT AND DIRECTIVE/POLICY

I INTRODUCTION TO SYSTEM SECURITY
- A. Purpose for System Security Plan and Program
- B. Goal, Objectives, and Tasks
- C. Scope of Program
- D. Security and Law Enforcement
- E. Management Authority and Legal Aspects
- F. Government Involvement
- G. Definitions Within 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 SYSTEM SECURITY PLAN
- A. Responsibility for Mission Statement and System Security Policy
- B. Management of Program
- C. Division of Security Responsibilities
- D. Proactive Security Committee
- E. Security Breach Review Committee

IV SYSTEM SECURITY PROGRAM: ROLES AND RESPONSIBILITIES
- A. Planning
- B. Proactive Measures
- C. Training
- D. Day-to-Day Activities

V THREATS 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
  2. External Audits

VII MODIFICATION OF SYSTEM SECURITY PLAN
- A. Initiation
- B. Review Process
- C. Implementation of 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.

FIGURE 1 Outline of transit system security program plan.

property, procedures, and environment of the authority, is known as system security. The plan should define and implement a system security program.

Goal, Objectives, and Tasks

Readers of the plan will want to know what it is expected to do. The primary goal, of course, is to implement a program consistent with the policy providing for system security. In this section, broad yet authority-specific objectives supporting that goal should be identified. In addition, each of the objectives should have associated with it a set of specific tasks that are well thought out, reasonable, and attainable.

A sample objective may be to develop an information system that logs all security breaches to support analysis and effective decisions. A sample task associated with this objective could be ensuring that the record-keeping system is able to log incidences by date, location, type, and disposition.

Scope of Program

The scope subsection of the plan should summarize the intent of the program, who is involved (and their functions), what organizations are affected, and what aspects of the system (presumably all) are affected. The scope should clearly relate to the objectives established previously.

Security and Law Enforcement

Transit authorities should take a proactive approach to security. Security breaches, however, will still need to be handled. The authority may rely on its own security forces, private companies, or sheriff's departments to react to security breaches. The plan should discuss here the relative roles of the law enforcement and transit security, including how they work together, communicate, and share jurisdictions.

Management Authority and Legal Aspects

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

Government Involvement

Most systems depend heavily on supplemental federal, state, and local funds. Include in the government subsection information on the specific sources of all major funding and explain security impacts due to the terms and conditions of the grants. For example, federal rules on third-party contracting regarding record keeping might affect the number of security companies willing to offer security capabilities.

Definitions Within Plan

Various transit and security terms should be defined so that the document will be clear and consistent to all readers. The authority may choose to write general descriptions of the various security concepts in the definitions subsection and to include more detailed formal definitions in an appendix.

TRANSIT SYSTEM DESCRIPTION

The plan will be of interest to many people, not only those familiar with the system. Although the document should be designed as a working tool for transit personnel, it may also be used as a reference by board members, city planners, nontransit police, citizens' interest groups, and government officials. Readers should need to look no farther than the plan itself to understand the nature of security within the system. This section of the plan will describe the transit system for which the plan has been created. Consequently, it will succinctly summarize the passenger, vehicle, and facility components; the operating environment; the role of the safety plan; and existing security conditions, following the outline shown in Figure 1. Most of this material need not 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.

In developing this section of the plan, remember that the plan is being developed with a systems approach. 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 elements of a system are diverse and interactive. Thus the system description must be comprehensive. Consider this big picture and the myriad potential audiences as the description of the transit system is developed.

The transit system description should include subsections addressing the following:

- 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.
- Organizational structure: define the various functional portions of the transit agency administration.
- Human resources: summarize the number of employees, their skills, and the way in which they are divided among the various functional entities within the agency.
- Passengers: describe the passengers that the authority serves, including demographic, population, and ridership information.
- Transit services and operations: introduce the various modes of travel services provided by the agency with summary information about the amount of exposure that they face in terms of hours.
- Operating environment: round out the reader's understanding of the system with narrative information about traffic, weather, geography, crime rates, and any other characteristics that describe the local environment.
- Facilities and equipment: provide appropriate information on the various facilities and equipment owned and operated by the authority.

Passenger, Vehicle, and System Safety Plan and Program

Over several years, FTA, through its research arm, the Volpe National Transportation Systems Center, has recommended that each authority develop a passenger, vehicle, and facility system safety plan and program. There are fundamental differences between safety and security. Safety is freedom from accidental danger, whereas security is freedom from intentional danger. The structure of the plan should be very similar to the safety plan, except that the concerns are not with accidental situations, but with deliberate actions taken by perpetrators to steal or damage property, harm people, or disrupt operations. This subsection of the plan should summarize the overall philosophy of the safety plan and program and integrate it with the security plan and program.

Current Security Conditions

The transit system description should also develop a portrait of current security conditions. Summarize the kind of security breaches that have occurred and are being addressed by this plan. Include documentation on the frequency of problems experienced during the previous year and other previous periods. Examples of security breaches may include, but are not necessarily limited to,

- Assault and battery
- Bomb scares
- Computer data base intrusion
- Disorderly conduct
- Drug abuse and sales
- Exhibitionism
- Facility and equipment damage
- Fare evasion and dodging
- Graffiti
- Lewdness
- Mugging
- Rape
- Sabotage, destruction, and altering
- Stock/parts shrinkage
- Terrorism
- Theft
- Trespassing
- Vandalism

The authority may want to develop a comprehensive list of security breaches and demonstrate, in a frequency-of-occurrence table, that it is free of some security problems. By identifying problems experienced by similar transit authorities that could arise locally, the authority prepares itself to address potential security problems.

Existing Security Capabilities and Practices

A subsection should summarize what is being accomplished by the authority to maximize security, including both proactive and responsive measures. In this subsection summarize the major proactive methods, procedures, devices, and systems that currently exist to prevent or minimize security breaches. They may include committee work, analysis, training programs, passenger coaching, and proactive security equipment.

For example, the authority may have created a proactive security review committee responsible for identifying potential and existing problem areas, developing standard operating procedures, and installing security devices. If the proactive security committee has been asked in previous periods to address certain issues, those measures should be included here. If the authority has developed data bases on security breaches, then the analysis of the collected data, the conclusions drawn, and the activities that have been implemented to improve security should be discussed. Information on any security-related training that has been completed by authority personnel should be noted. Training might, for example, include such courses as those offered by the Transportation Safety Institute in Oklahoma City related to terrorist threats such as bomb scares. Any passenger coaching that the authority has accomplished should be reported, such as exhorting passengers through advertising to closely guard their belongings at all times. Use of intrusion alarms, motion detectors, and other devices on facility entrances should be discussed.

The authority should also try to include the law enforcement community in proactive, preventive activities, and a description of those activities and the benefits realized should be discussed here as well.

No matter how proactive the authority, there will still be some security breaches. The capabilities of the authority and other law enforcement agencies to respond to a security breach on the transit system should be discussed.

MANAGEMENT OF SYSTEM SECURITY PLAN

Another section of the plan should account for each of the following security management functions:

- Developing the mission statement and overall system security policy,
- Managing the security program,
- Assigning specific responsibilities to staff, and
- Establishing proactive security and security breach review committees.

This section may therefore follow the outline originally shown in Figure 1.

Responsibility for Mission Statement and System Security Policy

A successful security plan requires leadership from the top of the organization and involvement at all levels. The plan should therefore identify who develops and signs the mission statement—usually an executive director or managing board—and who is responsible for setting security policies.

Management of Program

There are basically two structures for managing a security program. In smaller systems, the transit system manager has many responsibilities, including overseeing the program and carrying it out on a daily basis. In larger systems, the transit manager is ultimately accountable for system security but is more removed from daily operations; thus, it is likely that another individual would coordinate the daily activities of the program. This portion of the plan should state which management structure the system uses for its program and assign the following management activities:

- Ultimate responsibility for secure transit system operations;
- Communication of security as a top priority to all employees;
- Development of relations with outside organizations that contribute to the security program and with investigatory agencies such as the National Transportation Safety Board;
- Appropriate action on all security concerns brought to his or her attention;
- Identification of potential security concerns in any part of the system's operations;
- Active solicitation of the security concerns of other employees;
- Liaison between the proactive security and security breach review committees and transit system employees; and
- Assurance that the plan is carried out on a daily basis.

Division of Security Responsibilities

The plan should list all major positions within the security organization and their respective responsibilities, starting on a new page for each function to allow for easy revisions. For each position, summarize the overall security responsibilities, place those responsibilities in the context of the position's other work activities, and include a list of security-related tasks.

Proactive Security Committee

A proactive security committee should be created. Its major task is to identify and neutralize potential security problems before they happen. The committee should conduct system-wide security assessments, make sure that new procedures and facilities incorporate security in their design, develop and review training programs geared to security, look for new techniques that will improve security, and actively promote improved security awareness. This committee should also be responsible for security reviews that determine compliance with management policies, rules, regulations, standards, codes, and procedures.

The people who serve on the proactive security committee should represent various parts of the transportation organization and the local community. Having five to seven members allows the committee to possess a broad representative base and to retain manageability. Outside members could include representatives from the local police department, local officials, board members, and concerned leaders of community organizations. At monthly meetings members should report on security-related concerns, review potential problems, and designate individual members to investigate security issues. Once a security concern is brought to the attention of the committee, representatives should be chosen to evaluate the potential problem.

Security Breach Review Committee

A security breach review committee should also be established to identify and investigate actual security breaches to understand the deficiencies of the security program. Whereas the proactive committee seeks to prevent security breaches, the breach review committee looks at incidents that have already happened. In smaller transit systems, the two committees may be combined as a single security committee.

The incidents that the breach committee investigates may be controversial or sensitive. Therefore, the committee members must be objective individuals trusted by management and other employees. The committee members should include management, nonmanagement, and persons from outside the transit system.

The committee should review security incidents to determine whether the breach occurred because of incorrect policies or procedures, the failure of staff to carry out procedures, an accepted risk, unforeseen technology or action against the system, or some combination of these reasons. The committee may be able to recommend specific actions to prevent future security breaches of a similar nature or may refer a security breach to the system manager or the proactive security committee and ask them to develop preventive measures. The plan should spell out the extent of the authority of the breach committee in recommending actions or changes in security policy.

SYSTEM SECURITY PROGRAM: ROLES AND RESPONSIBILITIES

Individuals throughout the system will accomplish the overall security goals and objectives only if they are assigned roles and responsibilities in the form of procedures. A section of the plan should outline all of the regular security activities of the 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. These components may be organized according to the outline shown in Figure 1.

In many ways, this might be called the procedures section; it should be very specific, including tasks, assignments, standard operating procedures, and emergency operating procedures. The level of detail with regard to actual procedures means that the plan must be kept open and revised. The system must be willing to update the plan as ongoing activities change. It should combine those activities already being conducted and those to be implemented.

Each task must also be assigned to a specific position responsible for its accomplishment. This aspect of the security program cannot be overemphasized. "Roles and responsibil-

ities" is included in the title of this section to emphasize the need for people to take responsible action. Were the plan to consist only of procedures, there would be no guarantee that any tasks would be carried out, nor that any objectives would be accomplished.

Planning

The subsection on planning should outline all security planning activities and assign those functions to individuals. After the development of the first plan, most planning activities either will be ongoing or will grow out of the process of identifying, assessing, and resolving security threats and vulnerabilities. Regular planning activities might include meeting with the local chief of police annually to discuss long-term issues, reviewing the success of the security committees, establishing monthly security planning meetings with managers, and soliciting ideas from all staff for improved security.

The system's board of directors will play a role in the planning of security activities by way of approving the initiative to develop a plan and by reviewing and approving the plan. It should be made clear that the board may also assist in security planning by communicating any particular security concerns to top management. Security might also be placed on the board's agenda at a regular interval.

General planning responsibilities (probably relegated to the general manager or lead security officer) 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, and serving on the proactive security committee.

Other managers and supervisors have a wealth of understanding of the operation of the system and should be consulted by the security staff and committees. Managers should also 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.

All other staff can assist in security planning by sharing their security concerns and ideas for improvement through a supervisor, suggestion box, or appropriate security staff.

Proactive Measures

Proactive measures may be developed at the time of writing the plan to address recently discovered security problems, especially in the case of the first plan. Other proactive measures may have been recommended by the proactive security committee, or may have been only recently implemented. Because the system will not always want to wait until the next plan revision to implement proactive measures, some may be in full swing by the time of the update.

Briefly describe the problem each new proactive measure is designed to mitigate and the proactive measure, then assign responsibilities for each. Proactive measures that establish new operating procedures may refer to those procedures as presented later in the section on day-to-day activities. Yet-to-be implemented proactive measures should also include the implementation tasks necessary to initiate the new measures.

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. Security "training" may be as little as discussing security during all regular training programs or as much as sending staff to national workshops on transit security. This subsection should describe all training conducted in the interest of increased security, whether proactive or responsive, referencing any appropriate training documents; include detailed descriptions of training for security staff. This subsection should also describe all new training required to implement any new proactive training measures.

Day-to-Day Activities

Since the subsection on day-to-day activities will describe transit procedures in detail and the security program and plan are being developed using a systems approach, this subsection should be of significant size. It should consist of standard operating procedures (SOPs) and emergency operating procedures (EOPs). This subsection will be more specific than the earlier ones that described programs and responsibilities.

SOPs are the daily activities and tasks intended to accomplish any function within the transit system. They usually comprise the rules and policies of the transit system. Those that affect or are affected by security need to be described here and include, but are not limited to, such activities as

- Operators' leaving the vehicle for breaks and at the end of shifts;
- Securing of the building, lots, and yards at the close of business;
- Distribution of facility keys and assignment of access;
- Termination of employment;
- Collecting and counting revenue;
- Patrolling of facilities;
- Daily activities of security staff;
- Response to potential security breaches;
- Security-related activities of station attendants, train operators, and drivers; and
- Operator procedures for handling threats.

EOPs are the special procedures for nonroutine but serious occurrences, such as responding to alarms. EOPs also include contingency plans for nonpredictable occurrences that may have critical consequences, such as power failures or natural disasters. This subsection should detail the responses to actual security breaches, as well as all other EOPs that may affect security, including at the very least:

- Emergency reporting
- Emergency handling by security staff
- Emergency actions by front-line staff

- Dispatcher responses
- System actions for
  - Minor security beaches
  - Crimes against passengers
  - Violent crime
  - Burglaries
  - Other specific security breaches
- Incident investigation
- Media communications
- Contingency plans for
  - Power failures
  - Natural disasters
  - Terrorism

The format for a set of operating procedures includes a separate page for each procedure, title, affected personnel, level of restriction, list of procedures, and highlighted changes (optional). They may be organized in any fashion that is clear to all readers.

THREAT AND VULNERABILITY IDENTIFICATION, ASSESSMENT, AND RESOLUTION

A transit system by its very nature is vulnerable in various ways, because it owns property in remote public spaces and collects money. Vulnerability is the susceptibility of the system to a particular type of security hazard. Vulnerabilities are things that the authority can take specific defensive measures to correct, 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 intent to commit personal assault and vandalism. A potential security problem exists when these two components, threat and vulnerability, coincide. It is impossible for a system to be completely secure, just as it is impossible for a system to be perfectly safe: security therefore becomes a process of risk management.

Many authorities discover that a lack of statistical and historical data on incidents frustrates attempts to resolve problems. This section of the plan should establish methods to collect and communicate security information so that threats and potential threats (vulnerabilities) may be identified, examined, and resolved appropriately.

Threat and Vulnerability Identification

The subsection on threat and vulnerability identification describes the methods that the system will use to identify its threats and vulnerabilities. It is necessary to identify separately the major vulnerabilities of the system and the threats to which the system is subject, so that assumptions about vulnerability do not hide the possibility of problems with threats. Once these are brought into focus, security resources can be applied to solve specific problems.

Security Testing and Inspections

The primary purpose of security testing and inspection is to assess the vulnerability of the system to a security threat. It can also enhance preparedness and promote security awareness.

A three-phase approach is recommended to evaluate security preparedness. The first phase should confirm equipment preparedness, ensuring that security equipment is operable and properly located. The second phase should assess the proficiency of employees in how and when to use the equipment provided. The third phase should evaluate complete security systems, with exercises requiring coordination between different areas. This phased approach reveals system deficiencies in a useful way. For example, personnel cannot perform well if equipment is not available in good repair.

Data Collection

Within the system, many sources of information can help a security manager allocate resources, including incident and breach reports, passenger complaints, and personnel records. The plan should identify these sources, prescribe procedures for accessing this information, and state limits on its distribution. It should also identify how sources of outside information such as local police reports and the U.S. Department of Justice *Uniform Crime Reports* are obtained and used.

An incident report that collects information about security incidents should include

- Date and time
- Location
- Transit mode affected
- Persons involved
- Narrative of incident
- Estimated cost of damage
- Service disruption
- Security action taken
- Supervisor

These simple reports should be completed at the lowest level possible. They should not be used in investigations but are to alert the security system to threats so that improvement actions can be taken.

Reports

Reports provide summary data concerning the security information that has been collected. The subsection on reports should describe the types of security report to be developed and their distribution. Periodic management reports provide upper management with summary information on security breaches, costs, and ongoing security projects. Statistical reports should be more detailed and used by security staff to determine where problems are occurring and to identify any trends. An incident and security breach data base with a few key indexed fields can provide sufficient information to satisfy special request reports. The plan should place limits on the distribution of the various reports because they will contain sensitive information.

Security Information Flow

Another subsection should describe how the security information will be stored and move through the transit system.

All security information should be sent to a central point. For small transit systems, this information can be kept in files and used periodically to review security performance and to produce statistical reports. In a large system, a security data base should be developed to store, analyze, and retrieve security information. The plan should describe who will receive what security information, considering the sensitivity of the information, its usefulness to the person receiving it, and alternative ways of making this information available.

Threat and Vulnerability Assessment

The security information collected and communicated must be analyzed to determine where the system is vulnerable and what threats are most likely. The plan here should assign responsibility for security assessment and describe how the information will be analyzed and describe what will be done with results.

Responsibility

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. The plan should describe minimum qualifications of the analysts, including security experience, knowledge of the system, familiarity with the community, and knowledge of statistical methods and their limitations. The system may wish to rotate responsibility to keep the direct experience level of the analyses high and current.

Data Analysis

It is necessary to describe how the information will be analyzed. Vulnerability and threat are the two major factors involved in this analysis, which can be performed by first listing all of the facilities and systems that make up the transit property. Next, across the other dimension of a matrix, all possible threats, identified in incident reports or from police sources, are listed. The susceptibility of each facility or system on the list to each threat is assessed. When the matrix is completed it will reveal where security problems are most likely.

Frequency and Severity

Once vulnerability has been assessed, there is a need to predict which threats are most likely to occur. The plan should direct that threat analysis be conducted separately from the vulnerability analysis, otherwise evaluators may focus only on perceived threats and not on the real vulnerabilities. The threat analysis should rank each vulnerability on the basis of the likelihood that the threat will occur and the severity of a potential breach. When a high threat coincides with high severity and high vulnerability, security should be focused on that area.

Threat and Vulnerability Resolution

Some threats may demand emergency response, others may require a long-term project, and still others may just be accepted with no action taken. A subsection will need to discuss the factors that go into making such decisions.

Emergency Response

The plan should identify the criteria that activate certain emergency responses. A policy should be set for the appropriate type of response to each type of threat, depending on specific conditions. The plan should also describe the mechanism for activating 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.

Breach Investigation

Describe how incidents will be investigated. The goal of a breach investigation is to determine what circumstances led to the breach. Breach investigations and resulting reports submitted to management for action should describe

- Breach
- Source of threat
- Location
- Equipment involved and its physical condition
- Human factors
  - –Conditions at time of breach
  - –Training and knowledge of procedures
  - –Performance during breach
  - –Injuries
- Environmental conditions
- Actions taken to mitigate breach
- Command and control effectiveness
- Probable cause
- Recommendations

Research and Improvements

The security analysis will sometimes reveal a problem requiring additional study to determine ways to manage the risk. New technology often offers security improvements that a progressive system can adopt to its advantage. The plan should provide criteria for undertaking long-term improvements.

Criteria should also be established for acceptance of a new system. It should be able to prove itself in terms of effectiveness in an area of vulnerability, cost with a rapid payback period, and life-cycle dependability. Demonstration periods should be used to verify all claims for the new system before a full commitment is made.

Furthermore, the plan should 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. Consideration of employees' proposals will also instill greater commitment.

Eliminate, Mitigate, or Accept

The plan should recognize that there are three possible alternatives in resolving security problems. The first is to take steps to eliminate the problem, through redesign, retraining, or change in procedure. Although preferable, this is frequently not possible with available resources. The usual choice is to mitigate the threat. In some cases the risk will just have to be accepted, when the threat is so remote that it is not likely or its impact on the system may not be sufficiently dangerous. The factors that go into these decisions should be specified in the plan.

IMPLEMENTATION AND EVALUATION OF SYSTEM SECURITY PROGRAM PLAN

A section of the plan will provide details on how the program plan itself will be implemented and how progress of implementation will be evaluated. This is crucial to the establishment of an effective security program. Implementation will require development of three subsections as shown in Figure 1.

The first time a plan is developed and implemented, the planning process will take somewhat longer than it will in future years when the framework of the program is already established and proactive security measures are being developed regularly by the proactive security committee. In modifying and implementing a program that is already in place, most of the plan is already written. If the program in place is effective, many of the changes and solutions will have already been worked out.

Implementation Goals and Objectives

Major goals and specific objectives should be established for the implementation of the security plan to ensure that all transit system personnel understand exactly how the security program affects them, that the program receives appropriate support from management, that the activities described in the plan are undertaken, and that the system has the tools necessary to carry out the plan.

The primary goal of implementing the security plan will, of course, be to establish (or modify) a system security program. Other goals will support the primary goal. The authority should adopt implementation goals appropriate to its own system. Some important goals are to describe clearly the system security program and to describe accurately the system, the context of the program, and the security activities.

Supporting objectives may be to ensure that the plan is comprehensive and complete, that all managers and supervisors understand the objectives of the program, and that the plan is current. Another supporting objective might be to evaluate the security plan.

Another goal that defines the implementation of the security plan is that of communicating the program to all affected persons. Supporting objectives would be to obtain concurrence from the board of directors, distribute the security 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. The plan should be distributed to managers and supervisors first, so that those supervising others will be completely familiar with the security program before full implementation is initiated. 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, SOPs for fare revenue collecting and counting should be established during the security planning process but should not be distributed to every employee. Abridged plans may be distributed to most staff.

Another important goal of implementing the plan is to ensure that all transit personnel have the means to accomplish assigned responsibilities. Understanding the specific changes that affect them most is key to this process. Supervisory staff must clearly explain these changes and provide staff with the necessary skills to perform new tasks.

During plan implementation, both the proactive security and security breach committees should be established. If the committees are already established, the membership and organization may be changed as necessary.

Implementation Schedule

To carry out implementation, a timeline with specific milestones should be developed on the basis of the implementation goals and objectives, proceeding chronologically from the completion of the security plan document to the beginning of the formal yearly plan modification process. The schedule should include specific dates for each implementation task.

Evaluation

Constant evaluation of the program will be necessary during implementation. The evaluation process should extend from the initial draft of the plan document 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. This section of the plan should briefly explain how implementation will be evaluated.

Internal Review

During the implementation stages, when roles and responsibilities are assigned and new programs 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 endeavor to step back and assess the effectiveness of implementation. Lead security staff may meet weekly during implementation to make use of this feedback and to smooth the implementation process. The security committees should evaluate the plan and its implementation as part of their regular agendas to ensure that priorities are appropriately addressed.

External Audits

Regulatory agency, peer group, or consultant reviews should take place after the program has been implemented but before the plan modification process has begun. Doing so will enable the external reviewers to evaluate the program during a normal state and allow lead security staff enough time to evaluate feedback and to prepare an effective modified plan. A subsection should identify the techniques that will be used to evaluate formally the program from outside the system. It should include a schedule for requesting external audits, contacting the executing organization, assisting evaluators, and discussing results.

MODIFICATION OF SYSTEM SECURITY PLAN

The plan is intended to be a living document that is used daily. The day after implementation activities are initiated, the plan will begin to be considered for modifications, but security officers should not devote their time to constant revision of the plan. The plan can be the depository of notes, sample forms, and memos. When the yearly revision of the plan occurs, the security officer should not have to go back and recreate history in order to update the document.

Initiation

The actual process for initiating modifications to the security program plan will be defined here. For example, the plan may state that distributed copies will contain a memo or form requesting that the readers or users provide comments on any part of the plan that they believe is inadequate or inappropriate. The plan may state that the security officer and his or 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. The plan should also identify the procedure to be used when a modification to the program needs to be implemented immediately.

Review Process

The actual process used by the security department and those individuals responsible for modifying the program plan needs to be discussed. For example, the proactive security committee could be tasked with reviewing the plan and comparing it with actual operational experience four times a year to identify necessary changes. Another approach might be to establish a small committee 9 months after approval of the existing plan that would modify it or identify necessary changes. Mechanisms for including changes suggested by other department heads or the general manager should also be delineated.

Implementation of Modifications

Modifications to the plan can be manifested in several ways. For example, new procedures, staff responsibilities, or forms may be considered to be of enough value to require immediate implementation. In such instances, appropriate pages of the plan can be revised, approval of their content sought and obtained, and the revisions disseminated to all recipients of the plan. Modifications that can be implemented without extensive training can be instituted on an ongoing basis under the direction of the lead security officer.

CLOSURE

The system security program plan should be a complete guide to establishing and maintaining a comprehensive security program for the authority and the system for which it is responsible: this includes people, property, procedures, and environment. 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.

When complete, the plan document will have

- Demonstrated management's commitment and policy on security;
- Introduced the concept of a system security program;
- Described the transit system;
- Established the management of the plan;
- Detailed the security program by assigning responsibilities;
- Explained how threats and vulnerabilities will be identified, assessed, and resolved;
- Portrayed how the plan itself will be implemented to establish or revise the program; and
- Described how the security plan will be evaluated and modified.

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

APPENDIXES

Appendix A: Bibliography

Including a bibliography of good publications related to transit security contributes to the usefulness of the plan and demonstrates that significant research was considered and that the concepts in the plan are in concert with industry standards.

Appendix B: Glossary of Security Terms

A number of different individuals can be expected to read the plan. A glossary of security terms will give all readers the information necessary to appreciate fully the plan's content.

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

A third appendix should define all security-related organizations to which the authority and its personnel belong. There

will also be organizations that are potential resources. The section should list all resources that are person-based.

Appendix D: Security Forms and Logs

When the initial plan is created, the authority may already be using a number of forms and logs in day-to-day operations. Forms should be acquired, catalogued, labeled, and included in this appendix and any logs should be listed. Forms and logs from other authorities may be included here as examples being considered.

Additional Appendixes

Since the plan will be tailored to meet the requirements of the local authority, any other appendixes that may be needed or useful can be included.

ADDITIONAL INFORMATION

More detailed guidelines will be available through William T. Hathaway, Volpe National Transportation Systems Center, Cambridge, Massachusetts.

ACKNOWLEDGMENTS

The KETRON Division of the Bionetics Corporation would like to extend its full appreciation to FTA, 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 and Judy Meade, FTA; Adelbert Lavery, Volpe; and Debra J. Haas, KETRON Division, Bionetics Corporation.

Publication of this paper sponsored by Task Force on Transit Safety.