Appendix I

Version: 10/1/2021

System Security Plan (SSP) and

Security and Emergency Preparedness Plan (SEPP)

Content

Page intentionally left blank

System Security Plan (SSP) and Security and Emergency Preparedness Plan (SEPP) Requirements

The new State Safety Oversight (SSO) Rule (Part 674) no longer specifically requires the system security plan (SSP) or the security and emergency preparedness plan (SEPP). However, the SSP is now included as part of the SSO program as a minimum standard for safety as part of the NJDOT SSO program all-hazards approach to the system safety program. The NJDOT SSO program continues to require the SSP documentation, but no longer has jurisdiction over the content of the SSP. The following SSP standard is provided as an example of the content of an SSP for the RTA/RFGPTS, under the jurisdiction of New Jersey.

Objective

This section sets forth the NJDOT SSO program's standard for the System Security Plan (SSP), which is to be developed and formally approved by the NJDOT SSO program. The SSP should identify the legislative authority that created the RTA/RFGPTS, (or an organization contracted by a duly authorized transit authority or other governmental agency), and a policy statement, endorsed by upper management, that embraces security. The plan should describe the controls that are used to coordinate, communicate, and maintain liaison with the NJDOT SSO Program on security matters.

Each RTA/RFGPTS annually submits (or makes available for review) its SSP and/or SEPP and subsequent revisions thereto, to the NJDOT SSO program for review and approval as a minimum standard for safety document. The CSO provides verification that the SSP and/or SEPP was reviewed within the reporting calendar year as part of the Annual Report (See Program Standard Section 4 for details). The Triennial Safety Program Audit includes an all-hazards approach with a focus on the overlap of the security with the safety program.

System Security Plan Example Contents

Example contents of an SSP developed for an RTA/RFGPTS operating under the NJDOT SSO Program is identified as follows:

At a minimum, the System Security Plan and/or Security and Emergency Preparedness Plan developed by the RTA/RFGPTS should:

(a) Identify the policies, goals, and objectives for the security program endorsed by the agency's chief executive;
(b) Document RTA/RFGPTSRTA/RFGPTS process for managing threats and vulnerabilities during operations, and for major projects, extensions, new vehicles and equipment, including the integration with the safety certification process;
(c) Identify controls in place that address the personal security of passengers and employees;
(d) Document RTA/RFGPTS process for conducting internal security reviews to evaluate compliance and measure the effectiveness of the SSP; and
(e) Documents RTA/RFGPTS process for making its SSP and accompanying procedures available to the oversight agency for review and approval.

Sample Format for System Security Plans

System Security Plan Introduction

An RTA/RFGPTS is primarily vulnerable to certain types of crimes, including vandalism, graffiti, pick pocketing and purse snatching, fare avoidance, trespassing, and other security-related problems; however, transit systems have become potential targets for acts of terrorism. It is, therefore, necessary to identify these security threats and reduce the system's vulnerability to them to a practicable level. To emphasize the importance of security in all aspects of an RTA/RFGPTS, a set of comprehensive security activities should be established and documented in the System Security Plan. The overall goal of the security program is to maximize the level of security afforded to passengers, employees, and property.

To be effective, the security aspects of the SSP/SEPP are oriented toward identifying potential security problems and implementing remedial and/or mitigating measures before security problems arise. It is also important to recognize the sensitivity of security-related plans and procedures, as they are tactical in nature, and treated with a reasonable degree of confidentiality. For this reason, the security elements of the SSP/SEPP identify items, which need to be considered, but does not provide specific tactical related information.

Security Policy Statement

The highest levels of RTA/RFGPTS management set forth its policy embracing security. The appropriate management approval is denoted by signature on the policy statement and circulation of the statement to all departments. As part of this section, top management provides direction to the agency for the development of an SSP/SEPP that encompasses RTA/RFGPTS security policy statement in all facets of its operations.

Purpose of Security Program

The SSP/SEPP must identify the purpose of the security program endorsed by RTA/RFGPTS Chief Executive. The purpose of the SSP/SEPP should ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events.

Goals and Objectives

This SSP/SEPP should identify the goals of the security and emergency preparedness programs endorsed by RTA/RFGPTS chief executive. Goals should be realistic and presented in qualitative terms.

Scope of Security Program

Provide the scope of the Security Program to cover all agency personnel and be applicable to all agency operations:

- Each department/function that supports an RTA/RFGPTS SSP/SEPP and cooperates in achievement of the SSP/SEPP security objectives; each RTA/RFGPTS employee cooperates with the system safety and security/police functions and provides security with any information requested to aid in any threat or vulnerability identification, assessment or resolution, and/or security investigation; and
- Accountability for security and emergency preparedness of the rail transit system rests with each employee, supervisor, manager, and director

The scope includes the coordination and integration of emergency response plans with the RTA/RFGPTS and jurisdictions in the system's service area.

Security and Law Enforcement

This section of the SSP/SEPP describes the approach used by the RTA/RFGPTS for security and law enforcement functions including management and support for the implementation of the SSP/SEPP. An overview of the RTA/RFGPTS Law Enforcement (Police Department) should be provided, along with an overview of the department's activities.

When the RTA/RFGPTS employs its own security (non-sworn) force or purchases security services from a private company, the plan should provide an overview of these security services and identify the cooperation with local law enforcement agencies in the transit system's service area.

Where Memorandum of Understanding (MOU's) exists, the SSP/SEPP should discuss what arrangements are in place. The RTA/RFGPTS should indicate how information regarding response to incidents, planning and deployment, joint operations, special events, and threat and crime information is shared.

Management Authority and Legal Aspects

This section of the SSP/SEPP describes the authority which oversees the operation and management of the RTA/RFGPTS, including its police/security function.

The section identifies the charter or legislation which created the rail transit system, and addresses the roles of the Board of Directors, General Manager, other executive leadership, and the manager of the security/police function in executing the SSP/SEPP. The roles and responsibilities of middle management and line personnel may be briefly introduced and described (i.e., management within the transit security/police function, as well as the roles of supervisors and operations and maintenance personnel).

The section briefly discusses the ordinances, codes, rules and other laws enforced on the rail transit system (i.e., felonies and misdemeanors applicable to RTA/RFGPTS service area, fare evasion, vandalism, unlawful entry (trespass) upon transit property or vehicles, interference with movement of or access to transit vehicles, disorderly conduct on transit property or in transit vehicles, and offensive physical contact with a transit passenger, employee, agent, security or police agency.

Government Involvement

This section of the SSP/SEPP describes how the SSP/SEPP interfaces with local, state, and federal authorities to ensure security and emergency preparedness for the RTA/RFGPTS.

This section of the SSP/SEPP introduces and briefly describes the local, state, and federal agencies with whom the RTA/RFGPTS coordinates for security and emergency preparedness. For example, at the federal level, the RTA/RFGPTS may coordinate with government agencies for funding support and to ensure compliance with security regulations and grant requirements. Federal partners may include: Federal Transit Administration (FTA), Federal Highway Administration (FHWA), Federal Railroad Administration (FRA), Department of Homeland Security (DHS), and its subsidiary bureaus, including the Federal Emergency Management Agency (FEMA) and Transit Security Administration (TSA).

Security Acronyms and Definitions

Identify all of the acronyms and definitions used in the SSP/SEPP.

System Description

Background & History of System

Briefly describe the system's characteristics. Include a description of when and how the transit system was established, history of service delivery, major milestones in the transit system's history, and the modes of service provided. A system map and reference to RTA/RFGPTS website should also be provided.

Organizational Structure

This section of the SSP/SEPP should provide organizational charts showing the lines of authority and responsibility as they relate to security and emergency preparedness.

Include the following information as part of the SSP/SEPP:

- Detailed organizational diagrams for the RTA/RFGPTS showing the title of each position.
- Detailed diagram of the structure of the security/police function identifying the key positions at all levels.
- Diagrams showing the relationship and lines of communications between the security/police function and other units of the organization.
- The relationship of the transit system to local political jurisdictions, including law enforcement and emergency management agencies.

Human Resources

This section of the SSP/SEPP provides a categorization and break-down of all employees and contractors who work for/on the RTA/RFGPTS.

(This information may be referenced to the responsible RTA/RFGPTS Department for review)

Passengers

This section of the SSP/SEPP provides a description of the ridership. Annual ridership statistics for the most recent year should be provided. Ridership may be broken down by mode of service and day of the week. Weekly and annual totals should be provided.

(This information may be referenced to the responsible RTA/RFGPTS Department for review)

Service and Operations

This section of the SSP/SEPP describes the RTA/RFGPTS operations and services. Information should be provided on the size, location, and function of the agency's physical assets including: maintenance facilities, offices, stations, vehicles, signals, and structures for all modes.

Operating Environment

This section of the SSP/SEPP describes the RTA/RFGPTS operating environment, including traffic conditions, rail alignment, weather, issues associated with special events or other activities, safety issues associated with the RTA/RFGPTS, and levels of crime in the communities served by the RTA/RFGPTS.

Integration with Other Plans and Programs

This section of the SSP/SEPP describes how the SSP/SEPP integrates with other plans and programs maintained by the RTA/RFGPTS, including the Public Transportation Agency Safety Plan (PTASP), Safety Certification Plan, Emergency Operations Plan, and other documents and programs that affect security and emergency preparedness.

Describe the interface of the Security Department in its role for the safety certification and sign-off process, used to verify the operational readiness of a new fixed guideway transit systems, major system modifications, system expansions, new equipment, and facilities, enabling the RTA/RFGPTS to consider the system safe and secure for operations, prior to entering revenue service. The process illustrates the use of checklists to record compliance to criteria, standards, specifications, codes, and recommended guidelines and practices.

Current Security Conditions

Provide a description of the current security conditions at the RTA/RFGPTS and the types of security incidents experienced by the RTA/RFGPTS and their frequency of occurrence. This section should describe current security conditions and issues at the RTA/RFGPTS including incidents of crime experienced on the system and relevant information on passenger perceptions of security. Crime data should be provided, documenting the most recent year for which it is available. The types of security incidents (including Part I and Part II offenses and ordinance violations) and their frequency of occurrence on the RTA/RFGPTS should be included. Additionally, this section should provide context for this information, including a comparison of

crime rates at the RTA/RFGPTS over time and/or a comparison of crime rates from the RTA/RTS with crime rates in the municipalities of the RTA/RFGPTS service areas.

Capabilities and Practices

This section of the SSP/SEPP should summarize the methods and procedures, devices, and systems utilized to prevent or minimize security breaches, including passenger education, campaigns, delay, detection, and assessment devices used to minimize security incidents throughout the RTA/RFGPTS. In preparing this section, the RTA/RFGPTS may consider theft and vandalism at stations, parking lots, and terminal locations; drug dealing at stations/facilities; fare evasion; disruptive behavior, etc.

SSP Management Activities

Responsibility for Mission Statement and System Security Policy

This section of the SSP/SEPP should define the authority and responsibility for RTA/RFGPTS Security Organization, including but not limited to, designating, and listing the individual(s) responsible for determining security policy on behalf of the RTA/RFGPTS, and for carrying out the activities of the SSP/SEPP, and defining the Security/Police functions' mission and role in the organization.

Describe the role of the General Manager/CEO in preparing, revising, reviewing, and signing the policy statement and the role of the head of Security/Police function and staff in preparing, revising, and reviewing the SSP/SEPP.

Management of the SSP Program

The SSP/SEPP should identify the person(s) with overall responsibility for transit security and emergency preparedness, including day-to-day operations, SSP/SEPP-related internal communications, liaison with external organizations, and identifying and resolving SSP/SEPP-related concerns.

The SSP/SEPP should be reviewed at least once each calendar year to determine if changes are required. In this section, the RTA/RFGPTS should address when during the calendar the SSP/SEPP will be reviewed. After the annual review has been conducted, all revisions to the SSP/SEPP should be completed and submitted to the NJDOT SSO program for review and approval. Each RTA/RFGPTS submits (or makes available for review) the SSP/SEPP directly to the NJDOT SSO program for review and approval.

Specifically, this section should address who is responsible for the following critical SSP/SEPP management activities, as a minimum:

(1) Defining ultimate responsibility for secure rail transit system operations.
(2) Communicating that security is a priority for all rail transit employees.
(3) Advocating for, and allocating security program resources; directing day-to-day security operational activities (including tactics, intelligence and analysis); and assessing security performance.

(4) Developing and explaining relations with outside organizations that contributes to RTA/RFGPTS security and emergency preparedness program.
(5) Developing relations with local, state and federal security-related agencies, including security oversight roles of FTA's State Safety Oversight and Project Management Oversight (PMO) programs, security oversight role of DHS TSA, and emergency preparedness roles of DHS, the state Agency of Homeland Security, the region's emergency management group or committee, and Urban Area Security Initiative, Point-of-Contact Working Group.
(6) Explaining the mechanism for bringing security concerns to the attention of the appropriate RTA/RFGPTS official or group.
(7) Identifying potential security concerns in any part of RTA/RFGPTS operations, through internal or external audits.
(8) Actively soliciting the security concerns of employees.
(9) Explaining the liaison between transit system employees and other security and emergency preparedness groups, committees and functions at the RTA/RFGPTS, for the purpose of addressing employees' security concerns.
(10) Ensuring RTA/RFGPTS security and emergency preparedness program is carried out on a daily basis.

Division of Security Responsibilities

Provide a listing of the system security related responsibilities of the personnel who work within RTA/RFGPTS Security/Police Department should be provided. This section should present a detailed description of the security/police function, including staff, the qualifications of the personnel, any planned short or long-term additions to the security organization's mission, and any additional staff which may be required. Specific roles and responsibilities should also be identified.

As part of the security organization, the RTA/RFGPTS should consider forming two committees: a Proactive Security Committee and a Security Breach Review Committee; the former responsible for identifying and neutralizing security risks; and the latter responsible for identifying security issues, investigation of incidents and development of corrective action (countermeasures). Both committees reside within RTA/RFGPTS Security/Police Department.

The Proactive Security Committee conducts system-wide security assessments and ensures that new procedures and facilities incorporate security in their design. The committee reviews training curriculum geared to security. Additionally, this committee determines:

- Compliance with management policies, rules, procedures and assigned security responsibilities
- Identifies organizational issues that may contribute to security incidents, or less effective response to incidents
- Actively promotes security awareness campaigns and award programs

Staffing of this committee should be a combination of RTA/RFGPTS and local community representatives.

The Security Breach Review Committee identifies security breaches and investigates these breaches to understand the deficiencies in the security program. Unlike the Proactive Security Committee, this committee focuses on incidents that have already happened. It is acknowledged that the breaches and incidents investigated by this committee are controversial and sensitive. Such incidents may involve violence, criminal activity, or wrong doing by RTA/RFGPTS staff.

The Security Breach Review Committee reviews security incidents to determine whether the breach occurred because of:

- Incorrect policies or procedures
- Staff not following procedures
- An accepted risk, unforeseen technology, or action against the RTA/RFGPTS

SSP Program Description

Planning

This section of the SSP/SEPP identifies the activities and programs in place at the RTA/RFGPTS to support planning for system security and emergency preparedness. Planning for the SSP/SEPP includes developing internal agency plans to address SSP/SEPP issues during operations, budgeting for system security and emergency preparedness functions, addressing security requirements in system design and safety/security certification for extensions and major projects, renovations and rehabilitations; and coordinating with local emergency management agencies and public safety agencies to ensure integration of the rail transit system into the response community plans for major incidents.

Organization

This section of the SSP/SEPP identifies the SSP/SEPP-related activities and programs and the ability to coordinate with external agencies. The RTA/RFGPTS should identify its Incident Command Management System (ICS) based on the National Incident Management System (NIMS) and the capabilities of the agency to respond to major crimes, terrorism and natural disaster emergencies. Capabilities should be coordinated and integrated with external jurisdictions and regional emergency preparedness plans.

Equipment

Provide a description of the equipment used to support implementation of the system security program. Equipment required to support its capabilities to detect, prevent, respond to and recover from security and terrorism events and to manage natural disasters should also be required.

Training and Procedures

Describe the system security program related training and procedures to ensure employee proficiency. Training typically addresses rules, polices, and procedures as well as many hazards in RTA/RFGPTS operating environment. An overview of the training applicable to the RTA/RFGPTS include, but not limited to; SOPs, EOPs, Safety Rules, Security Awareness,

Security Systems (Facilities and Vehicles), Emergency First Responder Training, Introduction to ICS/NIMS, Incident Command Training, Interagency Training, Weapons of Mass Destruction/Chemical, Biological, Radiation, Nuclear, and Explosive (CBRNE), CPR, Blood-Borne Pathogens, First Aid, and Hazardous Material Awareness. The RTA/RFGPTS must also identify the specific procedures for Homeland Security threat level changes.

Emergency Exercises and Evaluation

Describe the system security-related activities to ensure the conduct of emergency exercises and evaluation. These exercises should address RTA/RFGPTS response to incidents which may be intentional (bomb threats, fire/arson, security breaches, etc.), unintentional (hazmat spills, accidental property/vehicle damage, etc.), or naturally occurring (high winds, floods, snowstorms, etc.).

Threat and Vulnerability Identification, Assessment, and Resolution

Threat and Vulnerability Identification

This section of the SSP/SEPP describes RTA/RFGPTS methods and activities to identify security-related threats and vulnerabilities. Include the identification and prioritize RTA/RFGPTS assets based on security data collection and analysis in addition to:

- The value of the asset, including current and replacement value;
- The value of the asset to a potential adversary;
- Where the asset is located;
- How, when, and by whom an asset is accessed and used; and
- The impact, if there assets are lost, on passenger, employees, public safety organizations, the general public and the public transportation operation.

Threat and Vulnerability Assessment

Provide a description of RTA/RFGPTS methods and activities to assess the likely impacts of identified threats and vulnerabilities on the system and to identify particular vulnerabilities which require resolution. Once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular danger, and the extent to which corrective measures can eliminate or reduce its severity.

Responsibility for assessment of these threats and vulnerabilities is assigned to personnel qualified in security deployment practices. Threat and vulnerability assessment considers:

- Experienced personnel (with knowledge of the RTA/RFGPTS) to be responsible for security assessment
- Analysis of the RTA/RFGPTS, familiarity with the communities, and knowledge of statistical methods
- Dissemination of security information to interested organizations (Management, Local Police, etc.)

Threat and Vulnerability Resolution

This section of the SSP/SEPP describes RTA/RFGPTS development of response strategies, both short and long term, to prioritized vulnerabilities, including the decision process used to determine whether to eliminate, mitigate, or accept security problems. Based on the results of the assessment, the RTA/RFGPTS can identify effective countermeasures to reduce vulnerabilities identified as unacceptable to management. Countermeasures include physical security, planning, coordination with local law enforcement agencies, and training and security exercises.

Threat and vulnerability resolution as a minimum includes:

- The mechanisms for activating certain types of emergency response including those authorized to respond, what levels of response are possible, and the duration the emergency response is capable of being maintained
- The methods employed to investigate security breaches including the circumstances that led to the breach
- The in-depth research of threats and vulnerabilities to determine if the risk(s) can be managed, and to provide criteria for long-term improvements in identified security risk areas
- The considerations of alternatives associated with security problems including eliminating the problem through design, retraining or procedural changes; minimizing the problem by increasing surveillance, changing procedures; increasing the presence of security forces; or accepting the security risk in those instances where the incident likelihood is remote, or impact to the system is so minor that it does not warrant action.

Internal Security Audit Process

The Internal Security Audit Process, a formal process of managing a security program, ensures that all elements of the security program are in place and performing as required. The Internal Security Audit Process is the method used to determine if all organizational elements, equipment, procedures, and functions are performing as intended from a security perspective. Security management and good overall management are inseparable concepts. The audit process is be part of the program and includes an approved implementation plan using checklists. The plan contains, as a minimum, the following:

Audit Responsibility

The RTA/RFGPTS should identify the unit or divisions of responsibility for oversight of the

Internal Security Audit Process. The unit responsible for the conduct of the audit should not be the unit in charge of implementation of the items being audited.

Employee and Contractor Security Program

The RTA/RFGPTS should identify the program in place to ensure employee and contractor compliance with the security requirements applicable to RTA/RFGPTS and contractor on-site work activities at the RTA/RFGPTS or on its operating property.

Related to the Contractor Security Program, the RTA/RFGPTS issues written security procedures, conducts security orientation meetings, and monitors contractor employees on or near the RTA/RFGPTS.

The internal security audit includes the verification of employee and contractor security or security awareness training, certification, and retraining programs as appropriate. A periodic review of the programs verifies that instructions and course contents meet the expectations of the training and certification requirements.

Audit Reporting

The audit report, an official document, provides a working level status of system elements to all levels of management. As part of the formal reporting, the chief executive officer receives a departmental summary report.

The RTA/RFGPTS conducts internal audits in a cooperative manner and includes an administrative process for resolving problems or disagreements.

Audit Completeness

Audits should be done on a coordinated basis with full management support, on an ongoing basis rather than an annual basis. The RTA/RFGPTS includes the following elements, as part of the audit procedure:

- **Cycle/Schedule**. A three-year audit schedule must be developed, reviewed, maintained and updated to ensure that all SSP/SEPP elements are reviewed during the audit cycle. The audited departments know when to expect audits. Audits are scheduled to be unobtrusive. Unannounced inspections or spot audits are approved as part of the overall audit process with concurrence of general management.
- **Checklists**. A unit conducting an audit prepares a list of security items to be audited in advance and issues the checklist to the department, under review. Each department, subject to review, produces the necessary documentation. This does not preclude spot check of individual records such as maintenance records or personnel qualification records. A cooperative nature is maintained throughout the audit process.
- **Documentation**. A unit conducting an audit maintains the formal documentation of all aspects of the internal audit process. As part of the formal documentation, general management and respective departments receive all necessary reports.
- **Follow-up/Corrective Action**. Each audit report process includes a list of recommended corrective actions, as appropriate. Management approves the corrective actions to be tracked by the Safety and/or Security Department for compliance. Each corrective action item receives an implementation schedule and monitored to completion.

The RTA/RFGPTS submits appropriate reports, corrective action plans, and schedules for implementation to the NJDOT SSO program, regarding investigations, three year safety reviews, internal security audits, safety certification processes, and reviews performed by the NJDOT SSO program. The RTA/RFGPTS consolidates all corrective action items and monitors the open items to completion, providing the information in its monthly reports to the NJDOT SSO program.

Three Year Security Review

The NJDOT SSO program conducts an on-site review of the RTA/RFGPTS to determine the extent to which the RTA/RFGPTS is meeting the requirements of its safety program and includes the all-hazards overlap with public safety and emergency preparedness/management. In preparation for this review, the RTA/RFGPTS and NJDOT SSO program establishes a schedule including notification to the RTA/RFGPTS, conduct of a pre-review meeting with the RTA/RFGPTS, preparation of draft and final reports, and required corrective action plans by the RTA/RFGPTS, if required.

If following the review, the RTA/RFGPTS is required to provide a corrective action plan; the RTA/RFGPTS will have 30 days to provide the NJDOT SSO program with this plan. The plan will identify the issue or condition found during the review, planned activities or action to resolve the condition, and the responsible RTA/RFGPTS department for implementing the corrective action, and the schedule completion dates for implementation.

Modification of System Security Plan and Emergency Procedures

Initiation

This section of the SSP/SEPP provides a description of the process used to initiate revisions to the security plan and emergency procedures, gather input for the revisions, procedures for updating the security plan and associated procedures, and the identification of responsible person(s).

System Security Plan and/or System Emergency Preparedness Plan Review Process

Describe the process used to review and revise the security plan as necessary, including frequency of reviews, and responsible person(s). This section of the SSP/SEPP should identify RTA/RFGPTS process for making the SSP/SEPP and companying procedures available to the NJDOT SSO program for review and approval.

Implementation Modifications

This section of the SSP/SEPP describes the process for communicating, disseminating, and implementing new and revised procedures of the security plan to appropriate RTA/RFGPTS staff.

Reviews of RTA/RFGPTS SSP/SEPP

After approval of RTA/RFGPTS initial SSP/SEPP, the RTA/RFGPTS will conduct an annual review of its SSP/SEPP and update it as necessary to ensure that the SSP/SEPP is current.

SSP and/or SEPP Submittals from New Starts Projects

An RTA/RFGPTS New Starts project is required to submit to the NJDOT SSO program or make available for review, an SSP/SEPP and associated procedures/referenced materials at least 180 calendar days before beginning passenger service operations. The initial SSP/SEPP will be reviewed and approved by the NJDOT SSO program and adopted by the RTA/RFGPTS as part of the project's safety certification process. As necessary, the NJDOT SSO program may require

additional documentation as part of the review and may request meetings or teleconferences to address identified issues.

SSP and/or SEPP Readiness Review

Specific to New Starts Projects, Major Projects, or extensions, the NJDOT SSO program may conduct on-site Readiness Reviews to assess the capabilities of the RTA/RFGPTS to implement its safety program during passenger operations. This assessment may be conducted in conjunction with the NJDOT SSO program's review and approval of the initial SSP/SEPP submission.

Updates:

- March 5, 2018 – initial release with Version 1.0
- July 6, 2020 – modifications to remove the formal review via checklist and approval process; converted to a minimum standard for safety/safety program related control document.
- June 30, 2021 – updated to include verification of annual SEPP/SSP review by the RTA/RFGPTS as part of the Annual Report.
- October 1, 2021 – formatting and RTA/RFGPTS changes.