



As security is not a requirement under 49 CFR 674, the requirements listed in this appendix are part of the DRPT Program Standard and state requirements which each transit agency under DRPT's purview must address. These guidelines are meant to align with the overall Program Standard and where possible, reference specific sections of the Program Standard. This is not intended to be a standalone document.

1 Security and Emergency Preparedness Plan (SEPP)

1.0 Objective

This section identifies the minimum requirements for the Security and Emergency Program Plan to be developed and implemented by each RTA subject to oversight of DRPT. These requirements will remain in effect until DRPT releases new requirements/ revisions to this Appendix or the Program Standard overall.

The RTA shall perform reviews of the SEPP annually to determine whether it needs to be revised to meet changed conditions and requirements.

The RTA shall submit to DRPT any intended changes to the SEPP for review and approval by January 1 of each year. Within thirty (30) days of the RTA's submittal, DRPT will issue a response letter to the RTA indicating any changes or approval of the SEPP including the checklist used to conduct the audit (See **Appendix P: Certification that Rail Transit Agency System Security and Emergency Preparedness Plan Has Been Developed, Reviewed, and Approved**). All SEPP documents will be handled in accordance with SSI requirements described in section 11.2.

1.1 Security and Emergency Preparedness Plan Minimum Requirements

Each RTA must develop, implement, and maintain a written Security and Emergency Preparedness Plan that complies with the program requirements specified in this section. These requirements are based on FTA's *System Security and Emergency Preparedness Planning Guide*, issued in January 2003. FTA's guide addresses all of the activities specified in 49 CFR Part 659.23. In addition, compliance with this FTA guide is required for RTA's participating in the Transit Security Grant Program (TSGP), administered by the Department of Homeland Security, Preparedness Directorate, Office of Grants and Training (G&T). The program requirements also affirm the authority of the Transportation Security Administration (TSA) in the areas of rail transit security and terrorism preparedness.

At a minimum, the SEPP developed by the RTA must:



- Identify the policies, goals, and objectives for the security program and be endorsed by the chief executive of the RTA.
- Document the RTA process for managing threats and vulnerabilities during operations and for major projects, extensions, new vehicles, and equipment including integration with the safety certification process.
- Identify controls in place that address the personal security of passengers and employees.
- Document the RTA process for conducting internal security audits to evaluate compliance and measure the effectiveness of the system security emergency preparedness plan.
- Document the RTA process for making available its SEPP and accompanying procedures to DRPT for review and approval.
- Identify controls for the RTA Information Security program.

DRPT has authority and a Sensitive Security Information (SSI) program in place to protect RTA security documents against public disclosure. DRPT will also adhere to the RTA's rules and procedures for protecting security-sensitive documents and information against public disclosure, and will work with the RTA as needed to develop protocols for reviewing such documentation.

2 Internal Security Audits

Requirements

This section describes DRPT requirements for the internal safety audit program to be implemented by the RTA. DRPT will require the RTA to audit each element of the TASP, and the seven elements of the current SEPP structure for its internal safety and security audits.

As described in the SSPP and SEPP, the RTA must implement a process for the performance of ongoing internal safety and security audits to ensure the implementation of the RTA SSPP and SEPP, and to evaluate the effectiveness of these plans. Internal audits may not be conducted in a compressed period once every three years, or even once a year; rather, they must be conducted in an ongoing manner throughout each year of the three-year cycle. Internal audits of RTA functions must be conducted by an individual outside of the chain of command for that function to avoid a conflict of interest (e.g. personnel within the RTA's safety function may not conduct an internal audit of the RTA's safety department).

For security audits, any special provisions established by the RTA or DRPT to ensure the protection of these materials must be followed.

Schedule

The RTA must develop and submit to DRPT an internal security audit schedule, which addresses all seven (7) required elements of the SEPP over a three-year cycle, ensuring that all elements of the SEPP are audited in an ongoing manner and completed. At a minimum, annual updates of this schedule must be provided to DRPT, with the annual report discussed in Section 4.5 below, by February 15th of each year.

DRPT is also required to audit the same elements of the SEPP over a three-year period, and the



RTA may elect to coordinate the audit schedule with DRPT such that the internal audits take place concurrently to the DRPT audits. In instances when the RTA coordinates their internal audits to take place concurrent to the DRPT audits, the RTA and DRPT will work together to develop an ongoing audit schedule. Please see Section 5 regarding DRPT External Safety Audit process and the concurrent audit schedule for 2017-2020.

Checklists

The RTA must develop checklists and procedures for conducting each of the seven (7) required SEPP audits and the Sensitive Security Information program requirement. These materials must ensure sufficient criteria to determine if all audited elements are performing as intended. These checklists are independent and separate of DRPT SSO's SEPP audit checklists.

DRPT Notification and Submissions

If the RTA elects to conduct its internal security audits separately from DRPT, then not less than thirty (30) calendar days prior to the conduct of an internal security audit, the RTA must notify DRPT. Notification must be in writing and transmitted to DRPT via letter, email, or fax. Notification should include the time and location of the internal audit. DRPT may observe any and all internal security audits.

Minimum Requirements for Annual Report on the Internal Security Audit Process

Similar to the safety requirement in section four, by February 15th of each year, DRPT requires the RTA to submit an annual report to DRPT that documents the internal audits conducted for the previous year. The annual report must be accompanied by a formal letter of certification signed by the rail transit agency's chief executive, indicating that the rail transit agency is in compliance with its security and emergency preparedness plan.

If the rail transit agency determines that findings from its internal security audits indicate that the rail transit agency is not in compliance with its system SEPP, the chief executive must identify the activities the RTA will undertake to come into compliance. DRPT must review and approve all CAPs using the procedures specified in Section 8 of this document. The RTA may submit this report in electronic copy via email or in hard copy via mail or fax. For sections devoted to the results of security audits, any special provisions established by the RTA or DRPT to ensure the protection of these materials must be followed.

In addition to the annual report, by February 15th of each year, DRPT requires that the RTA submit a formal letter of certification, signed by the RTA's senior executive, stating that, based on the evaluation performed during the internal safety and security audit process during the previous year, the RTA complies with its SEPP.

3 DRPT Audits

As part of the audit of the implementation of the SEPP, DRPT will audit the following elements:

1. SEPP Program Purpose, Goals & Objectives, Scope, Authority
2. Accuracy of the Conditions Written in the System Description
3. SEPP Management Activities
4. SEPP Program
5. Threat and Vulnerability Identification, Assessment, and Resolution
6. Implementation and Evaluation of the SEPP
7. SEPP Review and Modification

4 DRPT Program Standard Updates

Upon completion of the review and adoption, DRPT issues the final SSPS to the RTAs with instructions for implementation. The RTA is required to acknowledge receipt of the SSPS by letter. Following receipt and within sixty (60) calendar days, the RTA's must submit its TASP to DRPT for review and approval.