

# Security and Emergency Management Audit

Report #2024\_20

## Executive Summary

Internal audits of safety and security programs are conducted to assure that established processes are being implemented as intended and that these established plans and procedures are compliant to applicable federal and state regulations.

This audit included an assessment of policies, plans, and procedures in place to implement programs for public safety, security risk management, information security, and emergency management. ADS System Safety Consulting, on behalf of the Audit Division, conducted an initial review of documentation and interviewed ST Staff members. Further review and additional audit interviews were performed by Audit Division staff.

As part of this audit, compliance with the following state and federal requirements was assessed:

- 49 CFR Part 673 (FTA requirements for Emergency Preparedness)
- 49 CFR Part 239 and Part 270 (FRA requirements for Emergency Preparedness)
- 49 CFR Part 1582 (Public Transportation and Passenger Railroad Security)
- 49 CFR Part 15 and Part 1520 (Protection of Sensitive Security Information)
- FTA OP-54 (Security certification requirements for FTA project “readiness for service”)
- FTA General Directive 24-1 Required Actions Regarding Assaults on Transit Workers
- TSA Security Directive 1582-21-01 Enhancing Public Transportation and Passenger Railroad Cybersecurity
- RCW 81.112.180 (requirements for rail fixed guideway emergency preparedness plans)
- Washington State Rail Safety Oversight Program Standard

The audit scope included the following functional areas:

- Emergency Management
- Public Safety
- Information Security
- Security Risk Management

## Audit Objectives

Our audit had three objectives which are captured in the following bullet points:

- Identify applicable federal and state requirements for security and emergency management and assess alignment of ST plans and policies to these requirements.

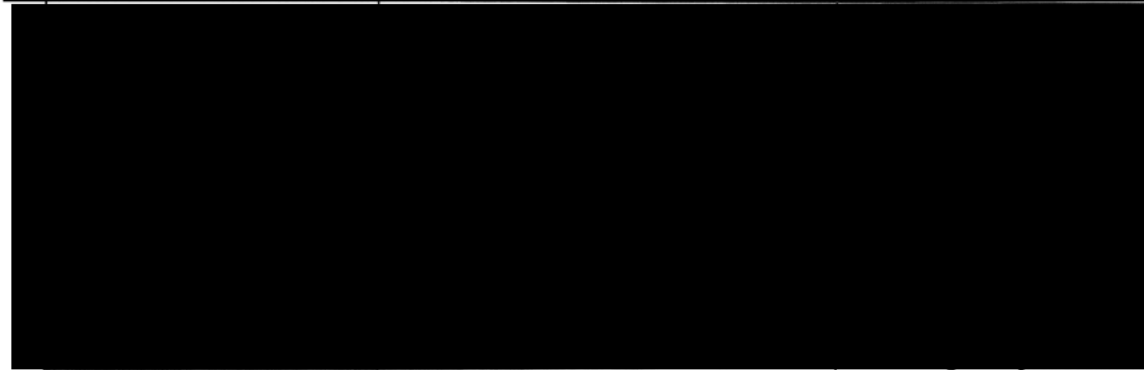
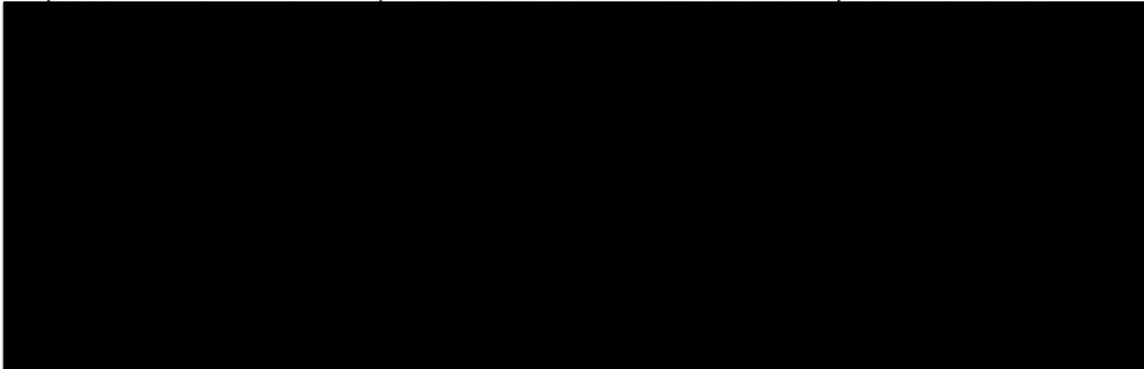
- To identify any program gaps, review roles and responsibilities for implementing ST security and emergency management plans and policies, including coordination between ST functional areas, partner agencies, and local jurisdictions.
- Identify any significant gaps where enhancements to plans, procedures or associated training should be made.

This audit period spanned from **April 2024** to **December 2024**.

## Conclusion

From our audit, we found **no findings** of non-compliance and **four (4) observations**; listed below:

Ref #	Description	Recommendation
O.1 (Risk Management)	Intergovernmental Agreements (IGA) do not consistently include clauses to allow for ongoing reviews, by <b>Information Security</b> of Operational Technology (OT) assets critical to revenue service operations.	Language for inclusion in future IGA updates should be drafted which requires ST Information Security to have access to conduct review and audit of OT assets critical to revenue service.



O.4 (Policy)	Due to limited SOPs, job aids, and training documents, there is a risk of programmatic knowledge loss in the event of <b>ST Public Safety</b> staff turnover.	Develop SOPs, job aids, and training documents to prevent programmatic knowledge loss in the event of ST Public Safety staff turnover.
--------------	---	--

## Background

There are no federal or state requirements for a single agency plan that covers Emergency Management, Public Safety, Information Security, and Security Risk Management for all modes and functional areas. Instead, there are recommended plans that equip Transit Agencies to meet FTA, FRA, TSA, and other requirements that fill specific business needs.

### Emergency Management, and Preparedness

The agency is moving to consolidate the Emergency Response Plan and the Emergency Management Plan into a single Emergency Operation Plan (EOP), applicable to all ST modes and functions. Significant progress has been made by the Emergency Management group to the draft EOP that achieves this goal of a single plan. Emergency Management is also responsible for overseeing familiarization training, tabletop and full-scale emergency exercises that meet FTA OP-54 Readiness for Service requirements and FRA 239.103 Passenger Train Emergency Simulations.

The Transportation Safety and Security group (TSS) maintains the System Security and Emergency Preparedness Plan (SSEPP) per requirements under RCW 81.112.180, CFR Parts 239, 270, and 673.

### Public Safety

The Public Safety group is responsible for overseeing contracted security operations and ensures that field operations are conducted according to contract specifications and established post orders, procedures, and plans. Field operations include security surveillance at revenue service locations such as stations and transit vehicles as well as non-revenue locations such as parking garages and operations and maintenance facilities. The Link Light Rail SSEPP also covers security operations for Link from an agency-level perspective. Public Safety also ensures that security concerns of ST staff are addressed through the reporting tool portal, security operations hotline, and on-site security details.

### Information Security

The Information Security Division (InfoSec) is responsible for conducting surveillance and reviews of critical Operational Technology (OT) assets and conducts vendor risk assessments on prospective vendors during the procurement process to ensure contract clauses reflect the appropriate security requirements for each procurement. A 2024 internal audit, *Vendor Management Follow-Up Performance Audit*, identified gaps in the procurement process where vendors are awarded contracts without necessary InfoSec review. InfoSec is working to expand

the coverage of its security program to all agency technology assets, including OT. Additionally, InfoSec maintains a Cybersecurity Incident Response Plan as required by TSA Security Directive 1582-21-01 Enhancing Public Transportation and Passenger Railroad Cybersecurity. This plan is maintained as an integral part of the agency's Information Security Management System (ISMS), established under Policy 1100.

### **Security Risk Management**

The Transportation Safety and Security group (TSS) is responsible for performing threat and vulnerability assessments (TVA) and security certification for the ST system. TSS follows the Safety and Security Management Plan and Safety and Security Certification Plan which meet the requirements of FTA OP-54 and the Washington State Rail Safety Oversight Program Standard. TSS conducts security reviews and assessments into revenue operations and prioritizes action plans based on security risk. TSS has developed physical security guidelines for the system and reviews and provides updates to the agency's Design Criteria Manual.

### **Method of evaluation and verification**

To assess compliance during the audit, the auditors completed the following steps:

- Identified and reviewed federal and state security requirements for applicability to ST.
- Reviewed organizational structure and ST agency policy for the management of security and emergency functions.
- Identified and reviewed policies, plans, and procedures that satisfy existing federal, state, and ST policy.
- Conducted interviews and reviewed documents supplied by ST staff to determine compliance with requirements (Appendix B contains the list of documents reviewed).

### **Audit Standards**

We performed our internal security audit according to Audit Division policies & procedures, which are governed by our Audit Charter; and meet several sets of applicable federal, state, and local auditing standards.

These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Phases

Each audit starts by examining the current processes in place relative to (1) laws or regulatory requirements, (2) agency policies and procedures and (3) industry best practices.

During the audit “planning” phase, we assess the engagement-specific conditions and risk, informing and confirming the audits’ objectives and scope. Also, relevant controls to mitigate these risks are also reviewed and identified.

The audit “field work” phase then examines the design of the identified controls to determine if the intent meets the regulations, policies, etc. If the controls are designed to adequately mitigate the risk (control environment), we move on to assess the degree to which the controls are mitigating the risk (control activities). Any areas identified where the control environment or activities do not adequately mitigate the identified risk are identified as an exception.

Exceptions are then defined as either findings or observations.

- **Findings** are the results of the evaluation and verification of evidence against audit criteria showing non-compliance with a policy, procedure, manual, standard, or industry best-practice.
- **Observations** are issues that may be compliant with requirements; however, the auditor has determined that the issue poses the potential risks of becoming a finding in the future if recommended changes are not put in place to prevent occurrence.

## Audit Results

There were no (0) findings and four (4) observations for this audit. The following table summarizes the observations using a Safety Management System (SMS) framework.

SMS Framework	Number of Findings	Number of Observations
Policy	0	1
Risk Management	0	3
Assurance	0	0
Promotion	0	0
<b>Totals</b>	<b>0</b>	<b>4</b>

## Audit Finding Details

We found no instances of non-compliance; No Findings resulted from this audit.

## **Appendices**

### **Appendix A: List of Interviewed staff**

The audit team interviewed the following individuals during this audit effort. Staff will be listed position title only:

Sound Transit:

#### **Transportation Safety and Security**

- Acting Chief Safety Officer
- Acting Director, Transportation Safety & Security
- Acting Director, Employee & Construction Safety
- Deputy Director, Investigations & Assessments
- Transportation Safety & Security Manager
- Sr. Transportation Safety & Security Specialist
- Safety Program Specialist

#### **Public Safety/Security**

- Acting Director, Public Safety
- Manager, Security Operations
- Manager, Public Safety & Security Field Activity
- Manager, Security Operations Center
- Public Safety Field Safety & Security Activity Supervisor (2)
- Sr. Security Specialist (2)
- Lead Security Specialist

#### **Emergency Management**

- Deputy Director, Emergency Management
- Emergency Management Manager
- Senior Emergency Management Specialist, Drills and Exercises
- Senior Emergency Management Specialist, Preparedness

#### **Design, Construction Management**

- Deputy Executive Director, Project Management Strategy

#### **Information Security**

- Chief Information Security Officer

## **Appendix B: List of Document Reviewed**

The following is a list of files reviewed as part of the audit:

### **ST Audit Team Document Review:**

2017-14 Adopting a Security, Law Enforcement, & Emergency Management Policy (Apr 2017)  
Construction Safety & Security Manual, Revision 5.1 (Sept 2024)  
Cyber Security Activation Plan (Mar 2024)  
Emergency Response Plan, Rev4 (Dec 2023)  
Continuity of Operations Plan (Nov 2024-DRAFT)  
Emergency Operations Plan, V2 (Nov 2024-DRAFT)  
InfoSec Activation Plan Milestone Schedule (Nov 2024)  
King County Hazard Identification and Risk Assessment Proposal (Nov 2024)  
Pierce County Hazard Identification and Risk Assessment Proposed Amendment (Nov 2024)  
Snohomish County-Sound Transit Hazard Identification and Risk Assessment (2024)  
Public Safety and Security Online Request Form (viewed Dec 2024)  
FTA General Directive 24-1: Actions Regarding Assaults on Transit Workers (Sept 2024)  
Washington State Rail Safety Oversight Program Standard,7.0 (Feb 2024)  
SSEPP revision internal memo from Branden Porter (March 2024)  
ST Operational TVA Master Schedule (viewed Dec 2024)  
Safety Security Assessment Template (TSS, viewed Dec 2024)  
Physical Security Design Guideline (Formerly PSSOP, TSS, Sept 2024-DRAFT)  
Safety and Security Management Plan, R8.0 (Mar 2022)  
Safety and Security Certification Plan, R4.0 (May 2023)  
Design Criteria Manual Revision 5, Amendment 11 (May 2021)  
TSA Security Directive SD 1580-21-01 Enhancing Rail Cybersecurity (Oct 2024)  
TSA Security Directive SD 1582-21-01 Enhancing Public Transportation and Passenger Railroad Cybersecurity (Oct 2024)  
System Security and Emergency Preparedness Plan, Version 5 (Dec 2023)  
NRV Fleet Plan (Apr 2024)  
NRV Fleet Safety Handbook (Nov 2023)  
Department Procedure 152A Semi-Annual Inspection Checklist (viewed Dec 2024)  
NDI Agreement for SSI (sampled process Dec 2024)

### **ADS Audit Team Document Review:**

Document List Available Upon Request

## Sound Transit's Title VI notice of rights

Sound Transit conducts Title VI equity analyses for service and fare decisions to ensure they are made as equitably as possible.

More information on Sound Transit's Title VI notice of rights and the procedures to file a complaint may be obtained by:

- Phone: 888-889-6368; TTY Relay 711;
- Email: [stdiscriminationcomplaint@soundtransit.org](mailto:stdiscriminationcomplaint@soundtransit.org);
- Mailing to Sound Transit, Attn: Customer Service, 401 S. Jackson St. Seattle, Washington 98104-2826; or
- Visiting our offices located at 401 S. Jackson St. Seattle, Washington 98104.

A complaint may be filed directly with the Federal Transit Administration Office of Civil Rights, Attention: Complaint Team, East Building, 5th Floor – TCR, 1200 New Jersey Avenue, SE, Washington, DC 20590 or call 888-446-4511.

### Report Prepared by:

**Mike Flood**

Digitally signed by Mike Flood  
Date: 2025.01.07 17:43:53  
-08'00'

---

Mike Flood, Sr. Compliance Auditor (Lead Auditor)

### Reviewed (QA/QC) by:

**Heather F.  
Wright**

Digitally signed by Heather F.  
Wright  
Date: 2025.01.08 10:05:21  
-08'00'

---

Heather Wright, Deputy Director, Audit Division

### Approved for release by:

**Patrick Johnson**

Digitally signed by Patrick  
Johnson  
Date: 2025.01.09 08:54:09 -08'00'

---

Patrick Johnson, Director, Audit Division