Region 5
Surface Operations Mission

Foster strong collaborative relationships with surface transportation stakeholders and engage with them to analyze their cyber and physical security programs to enhance security throughout the relevant industries.

TSA offers no-cost, voluntary programs through Structured Oversight that evaluate cyber and physical security postures of surface transportation stakeholders. TSA Surface Inspectors (TSIs) are assigned throughout Region 5 to conduct Structured Oversight activities.

- Las Vegas, NV
- Los Angeles, CA
- Oakland, CA
- Portland, OR
- Phoenix, AZ
- San Diego, CA
- Sacramento, CA
- Seattle, WA

TSA's duties extend far beyond our nation's airports. Surface TSIs ensure compliance with the Code of Federal Regulations and Security Directives, and provide Structured Oversight across multiple modes of surface transportation.

Surface Modes:

- Freight Rail
- Mass Transit/Passenger Rail
- Pipeline
- Highway
    - Over the Road Bus
    - School Bus
    - Trucking
- Maritime - TWIC

Region 5
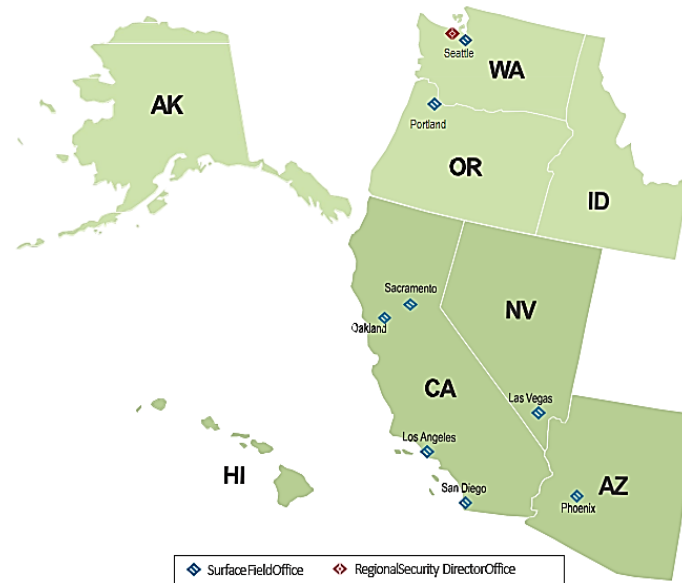
Surface Field Office   Regional Security Director Office

Contacts:

Regional Security Director:
James G. Duncan
James.G.Duncan@tsa.dhs.gov

Region 5 staff:
R5-Surface-Office@tsa.dhs.gov

Region 5 Cyber and Pipeline Team:
R5-Surface-Assessment-Team@tsa.dhs.gov

Surface Operations
Region 5

Transportation Security Administration

STRUCTURED OVERSIGHT |
BASE |
Baseline Assessment for Security Enhancement

BASE is a voluntary program that evaluates up to 21 aspects of the security programs for Mass Transit and Highway Motor Carriers (HMC). BASE assists entities establish and implement an enhanced security posture.

EXIS |
Exercise Information System

EXIS is a tabletop or full scale exercise that prepares an entity to effectively respond to security incidents. The exercise can be tailored to address the specific security interests of each entity.

SETA |
Security Enhancement Through Assessment

SETA is a collaborative program that is designed to evaluate and improve an entity's security posture at the front-line employee level. SETA includes three phases: the initial assessment, training, and a re-assessment.

T-START |
Transportation Security Template and Assessment Review Toolkit

T-START is a security plan template that assists HMC stakeholders and entities develop effective security plans. T-START is intended to strengthen prevention, protection, mitigation, response, and recovery capabilities among HMC stakeholders.

RMAST |
Risk Mitigation Activities for Surface Transportation

RMAST features risk reduction measures through engagement with industry stakeholders and the traveling public. Activities include: stakeholder engagement/training, and site security observations.

Pipeline Security Assessments |

Corporate Security Review (CSR) is a program that assesses a pipeline operator's physical security planning and implementation. The assessment enhances security preparedness and strengthens relationships that will be beneficial for the entity during a security-related event or emergency.

Critical Facility Security Review (CFSR) is an onsite assessment of physical security at critical pipeline facilities. Information collected from the review(s) is analyzed and used to determine strengths and areas for improvement in accordance to the TSA Pipeline Security Guidelines. TSA will revisit the agency at intervals of 6, 12 and 18 months from the date of the completed CFSR to assist with implementation of security recommendations.

Additional Training and Resources |

- TSA First Observer™ Plus
- IED/Explosive Recognition
- Active Shooter

Cyber Security |

Cybersecurity threats have become an increasing concern for TSA. Region 5 has a dedicated Cybersecurity team that works with entities on security directives/regulatory requirements, and leads outreach and structured oversight programs, to help stakeholders prepare for evolving cyber threats.

TSA offers free cyber preparedness resources.

- Cyber Security Evaluation Tool (CSET®) TSA (includes **Ransomware Readiness Assessment and TSA Validated Architecture Design Review**)
- Cybersecurity Baseline Assessment for Security Enhancement (Cy-BASE)
- Cyber Exercise Information System (EXIS)
- 5N5 - Five non-technical actions to consider in five days to enhance an entity's cybersecurity posture.

Regulatory Compliance |

- Inspections
- Code of Federal Regulations (CFR)
  - 1570-1584
- Security Directives (SDs)
  - Freight Rail
  - Public Transportation and Passenger Rail
  - Pipeline
- Investigations
  - Incident driven
  - Inspection driven