Chapter 310 Security

310.01 General
310.02 References
310.03 Design Considerations
310.04 MARSEC Levels
310.05 Vessel Security
310.06 Passenger Security Screening Area
310.07 Security Rooms
310.08 Toll Plaza and Vehicle Holding Area
310.09 Waterside Structures
310.10 Access Control/Restricted Areas/TWIC
310.11 Closed Circuit Television
310.12 Panic Buttons
310.13 Signage
310.14 Sensitive Security Information (SSI)

310.01 General

This chapter provides general guidelines for requirements from WSF Terminal Security personnel. Contact the WSF Company Security Officer (CSO) with any questions pertaining to security issues. For international terminals (Anacortes and Sidney) contact the local United States Customs and Border Protection (CBP) office to determine project specific requirements.

The *Terminal Design Manual* discusses secure terminal areas throughout the manual. Refer to the following chapters to find information on these secure areas:

Chapter	Subject
330	Marine
400	Passenger Buildings
430	Terminal Supervisor Buildings
570	Signage and Wayfinding
610	Vehicle Transfer Span
620	Passenger Overhead Loading

310.02 References

Unless otherwise noted, any code, standard, or other publication referenced herein refers to the latest edition of said document.

(1) Federal/State Laws and Codes

19 CFR, U.S. Customs and Border Protection, Department of Homeland Security; Department of the Treasury

33 CFR Chapter 1, Coast Guard Department of Homeland Security

33 CFR *Subchapter H Maritime Security*

33 CFR Part 165.1317 *Security and Safety Zone; Large Passenger Vessel Protection, Puget Sound and adjacent waters, Washington*

49 CFR Part 15 *Protection of Sensitive Security Information*

49 United States Code (USC) Chapters 401-501, Aviation and Transportation Security Act

International Port Security Program (ISPS Code)

Maritime Transportation Security Act (MTSA)

(2) Design Guidance

Design and Engineering Standards CG-521, United States Coast Guard (USCG)

Ferry Terminal Design Standards for Passenger Processing Facilities, United States Customs and Border Protection (USCBP)

310.03 Design Considerations

(1) Materials Specification

Utilize materials that are in accordance with the requirements of the WSDOT *Standard Specifications* and WSF *General Structural Notes* and *Regional General Special Provisions*. Consider the material requirements of federally funded projects including the requirement for American-made steel. Make use of WSF stockpiles of materials where possible.

(2) Proprietary Items

WSF uses competitively acquired products to fulfill the requirements of a contract wherever feasible to help achieve the lowest price, the best quality, and the most efficient use of resources. There are instances in which competitive bidding may not or cannot be provided and a specific proprietary product is allowed. Refer to Section 220.07(2) for limitations on the use of proprietary items.

310.04 MARSEC Levels

The United States Coast Guard (USCG) has a three-tiered system of Maritime Security (MARSEC) levels consistent with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC Levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. The Commandant of the

U.S. Coast Guard sets MARSEC levels commensurate with the HSAS. Because of the unique nature of the maritime industry, the HSAS threat conditions and MARSEC levels will align closely, though they will not directly correlate. It is the responsibility of the CSO to notify WSF of MARSEC level changes by issuing a Declaration of Security (DOS) to each terminal manager.

MARSEC levels are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

1. **MARSEC Level 1** means the level for which minimum appropriate security measures shall be maintained at all times. MARSEC 1 generally applies when HSAS Threat Condition Green, Blue, or Yellow are set.
2. **MARSEC Level 2** means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. MARSEC 2 generally corresponds to HSAS Threat Condition Orange.

3. **MARSEC Level 3** means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable, imminent, or has occurred, although it may not be possible to identify the specific target. MARSEC 3 generally corresponds to HSAS Threat Condition Red.

Consider the ability to adjust to changing MARSEC Levels in terminal design. Coordinate with the CSO for current security procedures and requirements in addition to potential new requirements that are expected over the design life of the terminal.

310.05 Vessel Security

Per 33 CFR Part 165.1317, "there is established a large passenger vessel security and safety zone extending for a 500-yard radius around all large passenger vessels located in the navigable waters of the United States in Puget Sound, WA, east of 123°30' West Longitude. [Datum: NAD 1983]." Consider requirements of the moving security zone, established by Captain of the Port Puget Sound, as follows:

- Vessels within 500 yards must operate at minimum speed necessary to maintain safe course and respond to directions of the WSF Watch Officer or on-scene official patrol officer.
- Vessels and persons are prohibited from approaching within 100 yards (underway) unless authorized by WSF or the on-scene patrol officer.
- Vessels and persons are prohibited from approaching within 25 yards of any WSF vessel docked at a terminal, without authorization.

310.06 Passenger Security Screening Area

Provide provisions in the passenger building for a passenger screening area that may be used during elevated security threat levels. Include provisions for power and communication outlets at this location. Coordinate with the CSO at the time of design for additional design recommendations associated with potential passenger screening requirements. Refer to Section 400.11 for more information.

310.07 Security Rooms

The following building spaces incorporated at WSF facilities serve security related functions. Refer to Chapter 430 for more information regarding the locations of these building spaces.

(1) Vessel and Terminal Security (VATS) Room

Provide an onsite office area for homeland security personnel and Washington State Patrol officers while security troopers are on duty at the ferry terminal, as needed. Coordinate with WSP and/or WSF Security in the early planning stages of design to determine if a VATS office is required. Allow enough space within the VATS room for two work stations with the exception of the Seattle terminal which requires four. Work stations include space for a computer, fax, copier, radio equipment, lockers, and telephone.

(2) Security Interview Room

Provide a security interview room for use by law enforcement personnel to conduct interviews and investigations at the following terminals:

- Seattle
- Fauntleroy
- Clinton

The need for security interview rooms is based partially on ridership and the response time of local police officers. Provide room with space to accommodate four persons with two table top check stations, computer, fax, copier, and telephone.

(3) Chemical Drug and Alcohol Testing

Provide a room for WSF Management to conduct chemical drug and alcohol testing. This room can be an employee-only restroom that is able to be temporarily closed to others so that testing can be conducted privately. Ideally, locate this restroom away from public areas and inside the terminal supervisor building.

(4) IT Equipment Network Room

The IT equipment network room is the central hub for terminal and revenue video monitoring, network ethernet, intercom dispersion and amplification, telephone interfacing, and terminal security and access equipment. Provide a location for network, phone, EFS and security equipment. Provide space for a minimum of two full size floor standing equipment racks with adequate room on either side of each rack for servicing equipment and enough room to provide an air conditioning unit sized to keep equipment at an ambient room temperature not to exceed 68 degrees Fahrenheit. Larger terminals such as Seattle, Bainbridge, Kingston, etc may require additional rack space. Consult WSF IT personnel for additional information.

The IT equipment network room also includes any needs for security equipment storage. Consider proving space to store portable security equipment that could be required for higher MARSEC level screening. Refer to Chapter 560 for additional design guidelines.

The IT equipment network room is designated as a critical restricted area (refer to Section 310.10).

310.08 Toll Plaza and Vehicle Holding Area

(1) Toll Plaza

There are no special security requirements associated with the toll plaza area. The toll booths serve as a revenue collection function and not a security function.

(2) K-9 Screening of Vehicles

The Washington State Patrol (WSP) is currently utilizing explosive sniffing K-9's at some terminals to screen vehicles within the holding area. Additional design requirements to accommodate these K-9's are not required.

(3) WSP Facility Parking

Parking spaces for WSP personnel is related to the number of work stations provided in the VATS room. Provide between 2 and 4 parking spaces based on terminal VATS requirements.

(4) Radiation Detectors

The use of radiation detection for vehicle screening purposes is not a WSF requirement. Radiation detectors are only used at WSF international terminals (i.e. Sydney and Anacortes) as mandated by U.S. Customs and Border Protection. Consult with the CSO and U.S. Customs and Border Protection Officials for design requirements.

(5) Fencing

Fencing is not required for security purposes at WSF terminals. During MARSEC Level 3 events, terminals facilities are required to be secure per USCG requirements. Fencing, when provided, can assist terminal personnel in meeting this requirement. In general, fencing provides a greater level of security, aids in emergency management, and can provide a means for revenue control.

Consider providing fencing at terminals where these factors are of concern. Refer to Section 500.09(2) for guidelines on revenue control fencing. Additionally, consider providing fencing in areas shown to have higher crime rates.

Design fencing, at a minimum, per the WSDOT *Design Manual* Chapter 560 for Type 3 fencing. Fencing may be required to be of custom type depending on intended function. At international terminals, coordinate with the WSF CSO and the local United States Customs and Border Protection (USCBP) office to determine project specific requirements.

310.09 Waterside Structures

(1) Trestle

There are no WSF security requirements associated with trestles. However, local city ordinances may have restrictions that apply to trestles. Contact the local jurisdiction to determine if any such ordinances/restrictions apply.

(2) Vehicle Transfer Span

Vehicle transfer spans require a security gate where vessels tie up overnight (refer to Chapter 330 for locations of WSF tie-up slips). The area seaward of the VTS gate is considered a critical restricted area when the gate is closed. Additional information on the type and location of VTS security gates is provided in Chapter 610.

(3) Passenger Overhead Loading

Pedestrian transfer spans require a security gate. The pedestrian transfer span is designated as a critical restricted area from the gate to the water outside of vessel loading and unloading. A TWIC card is required for access to a critical restricted area. Additional information on the type and location of OHL security gates is provided in Chapter 620.

(4) Wingwalls and Dolphins

There are no WSF security requirements associated with the wingwalls and dolphins.

310.10 Access Control / Restricted Areas / TWIC

Provide an access control system at the terminal. Design the access control system to be compatible and integrated with the Vigilos ESM software system. The access control system includes the following devices:

(1) Electronic Door Locks

Doors outfitted with these devices will be accessible by the use of an authorized employee proxy card ID, keypad or combination of both. Install these devices for rooms/areas that are considered a “Secure Area”. The access control system will monitor activities at all doors equipped with the electronic door locks and unusual events will be reported to the system operator.

(2) Key Locks

Install standard key type locks at all doors including those with and without electronic door locks.

(3) Intrusion Detection

Design all doors equipped with electronic door locks to report opening to the access control system. Provide closed circuit television cameras inside the buildings which include motion detection for intrusion when the buildings are unoccupied. In addition, provide motion detectors and silent alarms in secure areas to report intrusions to the access control system.

(4) Security Gates

Provide heavy duty steel security gates at each vehicle transfer span. Allow these gates to be capable of manual operation via an authorized employee proxy card ID.

(5) Roll Gates

Provide roll gates or doors at the vehicle transfer span and at the egress from the overhead loading near the passenger building.

310.11 Closed Circuit Television

Include a closed circuit television (CCTV) system at the terminal. This system is used for surveillance of public areas. WSF currently utilizes a Vigilos Enterprise Security Management (ESM) software system to manage its video and card access control systems. Design the CCTV to be compatible and integrated with the Vigilos ESM software system. Details of the CCTV system are considered SSI information. Coordinate with the WSF CSO if additional information is required for design.

310.12 Panic Buttons

Install panic buttons at the vehicle toll booths, passenger sales area, seller’s safe room, and the supervisor’s business and accounting room. Connect these to the terminal supervisor office for use by WSF agents in the event of an emergency at the toll booths.

310.13 Signage

The following security-related signage is incorporated at WSF terminals:

- MARSEC Level Signs are required at the entrance to the terminals in front of the toll booths.
- Signs indicating public areas are subject to video monitoring
- All vehicles subject to security screening and inspection
- Signage at the OHL transfer span stating that once loading has begun, the captain's permission is required to disembark the vessel.
- Terminal and vessel public areas are subject to video monitoring
- No Loitering/ Public Nuisance signs. Violators are subject to arrest.
- Employee Access Only
- Restricted Area
- No Trespassing
- Signs adjacent to trestle ladders

Refer to Chapter 770 for additional information.

310.14 Sensitive Security Information (SSI)

Sensitive Security Information (SSI) is that information defined in 49 CFR Part 1520 but also includes any information not specifically mentioned in Part 1520 but marked as "Sensitive Security Information" or "SSI". SSI includes all information obtained or developed in the conduct of security activities the disclosure of which the Transportation Security Administration, Department of Homeland Security has determined would be detrimental to the security of transportation.

SSI requires special handling to protect its secure nature. Plans and specifications containing SSI information require special headers and footers denoting the sensitivity of the information contained within the documents. Designers and contractors developing and handling SSI documents are required to sign a Non-Disclosure Agreement obligating them to protect this information from unauthorized disclosure. Refer to 49 CFR Part 1520 for the marking and handling of SSI documents.

Typically, if a document or contract includes SSI information, then the entire project is considered SSI. SSI projects can be more costly to design and construct due to the added requirements placed on a contractor for protecting the sensitive information. Hence it may be desirable to separate SSI work into a separate contract.