Coast Guard, another authorized Department of Homeland Security representative, or a Federal, State, or local law enforcement officer.

(f) There must be disciplinary measures in place to prevent fraud and abuse.

(g) Owners or operators must establish the frequency of the application of any security measures for access control in their approved security plans, particularly if these security measures are applied on a random or occasional basis.

(h) The vessel, facility, or OCS facility operator should coordinate the TWIC Program, when practical, with identification and TWIC access control measures of other entities that interface with the vessel, facility, or OCS facility.

[USCG–2007–28915, 81 FR 57709, Aug. 23, 2016]

§ 101.555 Recurring Unescorted Access for Risk Group A vessels and facilities.

This section describes how designated TWIC-holders may access certain secure areas on Risk Group A vessels and facilities on a continual and repeated basis without undergoing repeated electronic TWIC inspections.

(a) An individual may enter a secure area on a vessel or facility without undergoing an electronic TWIC inspection under the following conditions:

(1) Access is through a Designated Recurring Access Area (DRAA), designated under an approved Vessel, Facility, or Joint Vessel-Facility Security Plan.

(2) The entire DRAA is continuously monitored by security personnel at the access points to secure areas used by personnel seeking Recurring Unescorted Access.

(3) The individual possesses a valid TWIC.

(4) The individual has passed an electronic TWIC inspection within each shift and in the presence of the on-scene security personnel.

(5) The individual passes an additional electronic TWIC inspection prior to being granted unescorted access to a secure area if he or she enters an unsecured area outside the DRAA and then returns.

(b) The following requirements apply to a DRAA:

(1) It must consist of an unsecured area where personnel will be moving into an adjacent secure area repeatedly.

(2) The entire DRAA must be visible to security personnel.

(3) During operation as a DRAA, there must be security personnel present at all times.

(c) An area may operate as a DRAA at certain times, and during other times, access to secure areas may be obtained through the procedures in § 101.535.

(d) Personnel may enter the secure areas adjacent to a DRAA at any time using the procedures in § 101.535.

[USCG–2007–28915, 81 FR 57710, Aug. 23, 2016]

Subpart F—Cybersecurity

EFFECTIVE DATE NOTE: By USCG–2022–0802, 90 FR 6447, Jan. 17, 2025, subpart F was added, effective July 16, 2025.

§ 101.600 Purpose.

The purpose of this subpart is to set minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities to safeguard and ensure the security and resilience of the Marine Transportation System (MTS).

§ 101.605 Applicability.

(a) This subpart applies to the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR parts 104, 105, and 106.

(b) This subpart does not apply to any foreign-flagged vessels subject to 33 CFR part 104.

§ 101.610 Federalism.

Consistent with § 101.112(b), with respect to a facility regulated under 33 CFR part 105 to which this subpart applies, the regulations in this subpart have preemptive effect over a State or local law or regulation insofar as the State or local law or regulation applicable to the facility conflicts with these regulations, either by actually conflicting or by frustrating an overriding Federal need for uniformity.