Title 33 —Navigation and Navigable Waters
Chapter I —Coast Guard, Department of Homeland Security
Subchapter H —Maritime Security

PART 101—MARITIME SECURITY: GENERAL

Authority: 46 U.S.C. 70034, 70051, 70052, Chapter 701; E.O. 12656, 53 FR 47491, 3 CFR, 1988 Comp., p. 585; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; DHS Delegation No. 00170.1, Revision No. 01.3.

Source: USCG-2003-14792, 68 FR 39278, July 1, 2003, unless otherwise noted.

Editorial Note: Nomenclature changes to part 101 appear by USCG-2008-0179, 73 FR 35009, June 19, 2008.

Subpart A—General

§ 101.100 Purpose.

(a) The purpose of this subchapter is:

(1) To implement portions of the maritime security regime required by the Maritime Transportation Security Act of 2002, as codified in 46 U.S.C. Chapter 701;

(2) To align, where appropriate, the requirements of domestic maritime security regulations with the international maritime security standards in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI-2) and the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on 12 December 2002; and

(3) To ensure security arrangements are as compatible as possible for vessels trading internationally.

(b) For those maritime elements of the national transportation system where international standards do not directly apply, the requirements in this subchapter emphasize cooperation and coordination with local port community stakeholders, and are based on existing domestic standards, as well as established industry security practices.

(c) The assessments and plans required by this subchapter are intended for use in implementing security measures at various MARSEC Levels. The specific security measures and their implementation are planning criteria based on a set of assumptions made during the development of the security assessment and plan. These assumptions may not exist during an actual transportation security incident.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60470, Oct. 22, 2003]

§ 101.105 Definitions.

Unless otherwise specified, as used in this subchapter:

Alternative Security Program means a third-party or industry organization developed standard that the Commandant has determined provides an equivalent level of security to that established by this subchapter.

Area Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard Area as described in 33 CFR part 3.

Area Maritime Security (AMS) Assessment means an analysis that examines and evaluates the infrastructure and operations of a port taking into account possible threats, vulnerabilities, and existing protective measures, procedures and operations.

Area Maritime Security (AMS) Committee means the committee established pursuant to 46 U.S.C. 70112(a)(2)(A). This committee can be the Port Security Committee established pursuant to Navigation and Vessel Inspection Circular (NVIC) 09-02 series, available from the cognizant Captain of the Port (COTP) or at *https://www.dco.uscg.mil/Our-Organization/NVIC/*.

Area Maritime Security (AMS) Plan means the plan developed pursuant to 46 U.S.C. 70103(b). This plan may be the Port Security plan developed pursuant to NVIC 09-02 provided it meets the requirements of part 103 of this subchapter.

Area of Responsibility (AOR) means a Coast Guard area, district, marine inspection zone or COTP zone described in 33 CFR part 3.

Audit means an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient.

Barge means a non-self-propelled vessel (46 CFR 24.10-1).

Barge fleeting facility means a commercial area, subject to permitting by the Army Corps of Engineers, as provided in 33 CFR part 322, part 330, or pursuant to a regional general permit the purpose of which is for the making up, breaking down, or staging of barge tows.

Biometric match means a confirmation that: One of the two biometric templates stored in the Transportation Worker Identification Credential (TWIC) matches the scanned biometric template of the person presenting the TWIC; or the alternate biometric stored in a Physical Access Control System (PACS) matches the corresponding biometric of the person.

Breach of security means an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.

Bulk or *in bulk* means a commodity that is loaded or carried without containers or labels, and that is received and handled without mark or count. This includes cargo transferred using hoses, conveyors, or vacuum systems.

Bunkers means a vessel's fuel supply.

Canceled Card List (CCL) is a list of Federal Agency Smart Credential-Numbers (FASC-Ns) that have been invalidated or revoked because TSA has determined that the TWIC-holder may pose a security threat, or the card has been reported lost, stolen, or damaged.

Captain of the Port (COTP) means the local officer exercising authority for the COTP zones described in 33 CFR part 3. The COTP is the Federal Maritime Security Coordinator described in 46 U.S.C. 70103(a)(2)(G) and also the Port Facility Security Officer as described in the ISPS Code, part A.

Card Holder Unique Identifier (CHUID) means the standardized data object comprised of the FASC-N, globally unique identifier, expiration date, and certificate used to validate the data integrity of other data objects on the credential.

Card validity check means electronic verification that the TWIC has not been invalidated or revoked by checking the TWIC against the TSA-supplied list of cancelled TWICs or, for vessels and facilities not in Risk Group A, by verifying that the expiration date on the face of the TWIC has not passed.

Cargo means any goods, wares, or merchandise carried, or to be carried, for consideration, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel, facility, or OCS facility, except dredge spoils.

Cargo vessel means a vessel that carries, or intends to carry, cargo as defined in this section.

Carry-on item means an individual's accessible property, including any personal effects that the individual intends to carry onto a vessel or facility subject to this subchapter and is therefore subject to screening.

Certain Dangerous Cargo (CDC) means the same as defined in 33 CFR 160.202.

Checked baggage means an individual's personal property tendered by or on behalf of a passenger and accepted by a facility or vessel owner or operator. This baggage is accessible to the individual after boarding the vessel.

Commandant means the Commandant of the U.S. Coast Guard.

Company means any person or entity that owns any facility, vessel, or OCS facility subject to the requirements of this subchapter, or has assumed the responsibility for operation of any facility, vessel, or OCS facility subject to the requirements of this subchapter, including the duties and responsibilities imposed by this subchapter.

Company Security Officer (CSO) means the person designated by the Company as responsible for the security of the vessel or OCS facility, including implementation and maintenance of the vessel or OCS facility security plan, and for liaison with their respective vessel or facility security officer and the Coast Guard.

Contracting Government means any government of a nation that is a signatory to SOLAS, other than the U.S.

Cruise ship means any vessel over 100 gross register tons, carrying more than 12 passengers for hire which makes voyages lasting more than 24 hours, of which any part is on the high seas. Passengers from cruise ships are embarked or disembarked in the U.S. or its territories. Cruise ships do not include ferries that hold Coast Guard Certificates of Inspection endorsed for "Lakes, Bays, and Sounds", that transit international waters for only short periods of time on frequent schedules.

Cruise ship terminal means any portion of a facility that receives a cruise ship or its tenders for initial embarkation or final disembarkation.

Cruise ship voyage means a cruise ship's entire course of travel, from the first port at which the vessel embarks passengers until its return to that port or another port where the majority of the passengers disembark and terminate their voyage. A cruise ship voyage may include one or more ports of call.

Dangerous goods and/or hazardous substances, for the purposes of this subchapter, means cargoes regulated by parts 126, 127, or 154 of this chapter.

Dangerous substances or devices means any material, substance, or item that reasonably has the potential to cause a transportation security incident.

Declaration of Security (DoS) means an agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.

Designated Recurring Access Area (DRAA) means an area designated under § 101.555 where persons are permitted recurring access to a secure area of a vessel or facility.

Disembark means any time that the crew or passengers leave the ship.

District Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard District described in 33 CFR part 3.

Drill means a training event that tests at least one component of the AMS, vessel, or facility security plan and is used to maintain a high level of security readiness.

Electronic TWIC inspection means the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the stored biometric template.

Embark means any time that crew or passengers board the ship, including re-boarding at ports of call.

Escorting means ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted. This may be accomplished via having a side-by-side companion or monitoring, depending upon where the escorted individual will be granted access. Individuals without TWICs may not enter restricted areas without having an individual who holds a TWIC as a side-by-side companion, except as provided in §§ 104.267, 105.257, and 106.262 of this subchapter.

Exercise means a comprehensive training event that involves several of the functional elements of the AMS, vessel, or facility security plan and tests communications, coordination, resource availability, and response.

Explosives detection system means any system, including canines, automated device, or combination of devices that have the ability to detect explosive material.

Facility means any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or maintained by a public or private entity, including any contiguous or adjoining property under common ownership or operation.

Facility Security Assessment (FSA) means an analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.

Facility Security Officer (FSO) means the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers.

Facility Security Plan (FSP) means the plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels.

Ferry means a vessel which is limited in its use to the carriage of deck passengers or vehicles or both, operates on a short run on a frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service.

Foreign vessel means a vessel of foreign registry or a vessel operated under the authority of a country, except the U.S., that is engaged in commerce.

General shipyard facility means—

(1) For operations on land, any structure or appurtenance thereto designed for the construction, repair, rehabilitation, refurbishment, or rebuilding of any vessel, including graving docks, building ways, ship lifts, wharves, and pier cranes; the land necessary for any structures or appurtenances; and the equipment necessary for the performance of any function referred to in this definition; and

(2) For operations other than on land, any vessel, floating drydock, or barge used for, or a type that is usually used for, activities referred to in paragraph (1) of this definition.

Gross register tons (GRT) means the gross ton measurement of the vessel under 46 U.S.C. chapter 145, Regulatory Measurement. For a vessel measured under only 46 U.S.C. chapter 143, Convention Measurement, the vessel's gross tonnage, ITC is used to apply all thresholds expressed in terms of gross register tons.

Gross tonnage, ITC (GT ITC) means the gross tonnage measurement of the vessel under 46 U.S.C. chapter 143, Convention Measurement. Under international conventions, this parameter may be referred to as "gross tonnage (GT)."

Hazardous materials means hazardous materials subject to regulation under 46 CFR parts 148, 150, 151, 153, or 154, or 49 CFR parts 171 through 180.

High seas means the waters defined in § 2.32(d) of this chapter.

Identity verification means the process by which an individual presenting a TWIC is verified as the owner of the TWIC.

Infrastructure means facilities, structures, systems, assets, or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health or safety of the port.

International voyage means a voyage between a country to which SOLAS applies and a port outside that country. A country, as used in this definition, includes every territory for the internal relations of which a contracting government to the convention is responsible or for which the United Nations is the administering authority. For the U.S., the term "territory" includes the Commonwealth of Puerto Rico, all possessions of the United States, and all lands held by the U.S. under a protectorate or mandate. For the purposes of this subchapter, vessels solely navigating the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island and, on the north side of Anticosti Island, the 63rd meridian, are considered on an "international voyage" when on a voyage between a U.S. port and a Canadian port.

ISPS Code means the International Ship and Port Facility Security Code, as incorporated into SOLAS.

Maritime Security (MARSEC) Directive means an instruction issued by the Commandant, or his/her delegee, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.

Maritime Security (MARSEC) Level means the level 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.

MARSEC Level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

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 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 or imminent, although it may not be possible to identify the specific target.

Master means the holder of a valid merchant mariner credential or license that authorizes the individual to serve as a Master, operator, or person in charge of the rated vessel. For the purposes of this subchapter, Master also includes the Person in Charge of a MODU, and the operator of an uninspected towing vessel.

Merchant mariner credential or MMC means the credential issued by the Coast Guard under 46 CFR part 10. It combines the individual merchant mariner's document, license, and certificate of registry enumerated in 46 U.S.C. subtitle II part E as well as the STCW endorsement into a single credential that serves as the mariner's qualification document, certificate of identification, and certificate of service.

Mobile Offshore Drilling Unit (MODU) means the same as defined in 33 CFR 140.10.

Non-TWIC visual identity verification means the process by which an individual who is known to have been granted unescorted access to a secure area on a vessel or facility is matched to the picture on the facility's PACS card or a government-issued identification card.

OCS Facility means any artificial island, installation, or other complex of one or more structures permanently or temporarily attached to the subsoil or seabed of the OCS, erected for the purpose of exploring for, developing or producing oil, natural gas or mineral resources. This definition includes all mobile offshore drilling units (MODUs) not covered under part 104 of this subchapter, when attached to the subsoil or seabed of offshore locations, but does not include deepwater ports, as defined by 33 U.S.C. 1502, or pipelines.

Offshore Supply Vessel (OSV) means the same as defined in 46 CFR 125.160.

Operator, Uninspected Towing Vessel means an individual who holds a merchant mariner credential or license described in 46 CFR 15.805(a)(5) or 46 CFR 15.810(d).

Owner or operator means any person or entity that owns, or maintains operational control over, any facility, vessel, or OCS facility subject to this subchapter. This includes a towing vessel that has operational control of an unmanned vessel when the unmanned vessel is attached to the towing vessel and a facility that has operational control of an unmanned vessel when the unmanned vessel is not attached to a towing vessel and is moored to the facility; attachment begins with the securing of the first mooring line and ends with the casting-off of the last mooring line.

Passenger vessel means—

(1) On an international voyage, a vessel carrying more than 12 passengers, including at least one passenger-for-hire; and

(2) On other than an international voyage:

(i) A vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire;

(ii) A vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire;

(iii) A vessel that is chartered and carrying more than 12 passengers;

(iv) A submersible vessel that is carrying at least one passenger-for-hire; or

(v) A wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.

Passenger-for-hire means a passenger for whom consideration is contributed as a condition of carriage on the vessel, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person having an interest in the vessel.

Personal Identification Number (PIN) means a personally selected number stored electronically on the individual's TWIC.

Physical Access Control System (PACS) means a system that includes devices, personnel, and policies, that controls access to and within a facility or vessel.

Port of call means a U.S. port where a cruise ship makes a scheduled or unscheduled stop in the course of its voyage and passengers are allowed to embark and disembark the vessel or its tenders.

Public access facility means a facility—

(1) That is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104;

(2) That has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and

(3) That receives only:

(i) Vessels not subject to part 104 of this chapter, or

(ii) Passenger vessels, except:

(A) Ferries certificated to carry vehicles;

(B) Cruise ships; or

(C) Passenger vessels subject to SOLAS Chapter XI-1 or SOLAS Chapter XI-2.

Qualified Reader means an electronic device listed on TSA's Qualified Technology List that is capable of reading a TWIC.

Recurring unescorted access refers to special access procedures within a DRAA where a person may enter a secure area without passing an electronic TWIC inspection prior to each entry into the secure area.

Registered length means the registered length as defined in 46 CFR part 69.

Restricted areas mean the infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection. The entire facility may be designated the restricted area, as long as the entire facility is provided the appropriate level of security.

Review and approval means the process whereby Coast Guard officials evaluate a plan or proposal to determine if it complies with this subchapter and/or provides an equivalent level of security.

Risk Group means the risk ranking assigned to a vessel, facility, or OCS facility according to § 104.263, § 105.253, or § 106.258 of this subchapter, for the purpose of TWIC requirements in this subchapter.

Screener means an individual who is trained and authorized to screen or inspect persons, baggage (including carry-on items), personal effects, and vehicles for the presence of dangerous substances and devices, and other items listed in the vessel security plan (VSP) or facility security plan (FSP).

Screening means a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.

Secure area means the area on board a vessel or at a facility or outer continental shelf facility over which the owner/operator has implemented security measures for access control in accordance with a Coast Guard approved security plan. It does not include passenger access areas, employee access areas, or public access areas, as those terms are defined in §§ 104.106, 104.107, and 105.106, respectively, of this subchapter. Vessels operating under the waivers provided for at 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. Facilities subject to part 105 of this subchapter located in the Commonwealth of the Northern Mariana Islands and American Samoa have no secure areas. Facilities subject to part 105 of this subchapter may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure areas.

Security sweep means a walkthrough to visually inspect unrestricted areas to identify unattended packages, briefcases, or luggage and determine that all restricted areas are secure.

Security system means a device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.

Sensitive security information (SSI) means information within the scope of 49 CFR part 1520.

SOLAS means the International Convention for the Safety of Life at Sea Convention, 1974, as amended.

Survey means an on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.

Terminal screening program or TSP means a written program developed for a cruise ship terminal that documents methods used to screen persons, baggage, and carry-on items for the presence of dangerous substances and devices to ensure compliance with this part.

Transparent Reader means a device capable of reading the information from a TWIC or individual seeking access and transmitting it to a system capable of conducting electronic TWIC inspection.

Transportation security incident (TSI) means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

TWIC means a valid, non-revoked transportation worker identification credential, as defined and explained in 49 CFR part 1572.

TWIC Program means those procedures and systems that a vessel, facility, or outer continental shelf (OCS) facility must implement in order to assess and validate TWICs when maintaining access control.

TWIC reader means a device capable of conducting an electronic TWIC inspection.

Unaccompanied baggage means any baggage, including personal effects, that is not being brought on board on behalf of a person who is boarding the vessel.

Unescorted access means having the authority to enter and move about a secure area without escort.

Vessel-to-facility interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of facility services to or from the vessel.

Vessel-to-port interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, cargo, vessel stores, or the provisions of port services to or from the vessel.

Vessel Security Assessment (VSA) means an analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.

Vessel Security Plan (VSP) means the plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes, and persons on board at the respective MARSEC Levels.

Vessel Security Officer (VSO) means the person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel's Company Security Officer.

Vessel stores means—

(1) Materials that are on board a vessel for the upkeep, maintenance, safety, operation or navigation of the vessel; and

(2) Materials for the safety or comfort of the vessel's passengers or crew, including any provisions for the vessel's passengers or crew.

Vessel-to-vessel activity means any activity not related to a facility or port that involves the transfer of cargo, vessel stores, or persons from one vessel to another.

Visual TWIC inspection means the process by which the TWIC is authenticated, validated, and the individual presenting the TWIC is matched to the photograph on the face of the TWIC.

Waters subject to the jurisdiction of the U.S., for purposes of this subchapter, includes all waters described in section 2.36(a) of this chapter; the Exclusive Economic Zone, in respect to the living and non-living resources therein; and, in respect to facilities located on the Outer Continental Shelf of the U.S., the waters superjacent thereto.

[USCG-2003-14792, 68 FR 39278, July 1, 2003]

Editorial Note: For FEDERAL REGISTER citations affecting § 101.105, see the List of CFR Sections Affected, which appears in the Finding Aids section of the printed volume and at *www.govinfo.gov*.

§ 101.110 Applicability.

Unless otherwise specified, this subchapter applies to vessels, structures, and facilities of any kind, located under, in, on, or adjacent to waters subject to the jurisdiction of the U.S.

§ 101.112 Federalism.

(a) The regulations in 33 CFR parts 101, 103, 104, and 106 have preemptive effect over State or local regulation within the same field.

(b) The regulations in 33 CFR part 105 have preemptive effect over State or local regulations insofar as a State or local law or regulation applicable to the facilities covered by part 105 would conflict with the regulations in part 105, either by actually conflicting or by frustrating an overriding Federal need for uniformity.

[USCG-2007-28915, 81 FR 57708, Aug. 23, 2016]

§ 101.115 Incorporation by reference.

(a) Certain material is incorporated by reference into this subchapter with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in paragraph (b) of this section, the Coast Guard must publish notice of change in the FEDERAL REGISTER and the material must be available to the public. All approved material is on file at the Office of the Coast Guard Port Security Directorate (CG-5P), Coast Guard Headquarters, 2100 2nd St., SW., Stop 7581, Washington, DC 20593-7581, or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202-741-6030, or go to: *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.* All material is available from the sources indicated in paragraph (b) of this section.

(b) The materials approved for incorporation by reference in this subchapter are as follows:

International Maritime Organization (IMO)

Publication Section, 4 Albert Embankment, London SE1 7SR, United Kingdom.

Conference resolution 1, Adoption of amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974, and amendments to Chapter XI of SOLAS 1974, adopted December 12, 2002, (SOLAS Chapter XI-1 or SOLAS Chapter XI-2)	101.120; 101.310; 101.410; 101.505; 104.105; 104.115; 104.120; 104.297; 104.400.
Conference resolution 2, Adoption of the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on December 12, 2002 (ISPS Code)	101.410; 101.505; 104.105; 104.115; 104.120; 104.297; 104.400.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 69 FR 18803, Apr. 9, 2004; USCG-2010-0351, 75 FR 36282, June 25, 2010; USCG-2013-0397, 78 FR 39173, July 1, 2013]

§ 101.120 Alternatives.

(a) ***Alternative Security Agreements.***

(1) The U.S. may conclude in writing, as provided in SOLAS Chapter XI-2, Regulation 11 (Incorporated by reference, see § 101.115), a bilateral or multilateral agreements with other Contracting Governments to SOLAS on Alternative Security Arrangements covering short international voyages on fixed routes between facilities subject to the jurisdiction of the U.S. and facilities in the territories of those Contracting Governments.

(2) As further provided in SOLAS Chapter XI-2, Regulation 11, a vessel covered by such an agreement shall not conduct any vessel-to-vessel activity with any vessel not covered by the agreement.

(b) ***Alternative Security Programs.***

(1) Owners and operators of vessels and facilities required to have security plans under part 104, 105, or 106 of this subchapter, other than vessels that are subject to SOLAS Chapter XI, may meet the requirements of an Alternative Security Program that has been reviewed and approved by the Commandant (CG-5P) as meeting the requirements of part 104, 105, or 106, as applicable.

(2) Owners or operators must implement an approved Alternative Security Program in its entirety to be deemed in compliance with either part 104, 105, or 106.

(3) Owners or operators who have implemented an Alternative Security Program must send a letter to the appropriate plan approval authority under part 104, 105, or 106 of this subchapter identifying which Alternative Security Program they have implemented, identifying those vessels or facilities that will implement the Alternative Security Program, and attesting that they are in full compliance therewith. A copy of this letter shall be retained on board the vessel or kept at the facility to which it pertains along with a copy of the Alternative Security Program and a vessel, facility, or Outer Continental Shelf facility specific security assessment report generated under the Alternative Security Program.

(4) Owners or operators shall make available to the Coast Guard, upon request, any information related to implementation of an approved Alternative Security Program.

(c) ***Approval of Alternative Security Programs.*** You must submit to the Commandant (CG-5P) for review and approval the Alternative Security Program and the following information to assess the adequacy of the proposed Alternative Security Program:

(1) A list of the vessel and facility type that the Alternative Security Program is intended to apply;

(2) A security assessment for the vessel or facility type;

(3) Explanation of how the Alternative Security Program addresses the requirements of parts 104, 105, or 106, as applicable; and

(4) Explanation of how owners and operators must implement the Alternative Security Program in its entirety, including performing an operational and vessel or facility specific assessment and verification of implementation.

(d) ***Amendment of Approved Alternative Security Programs.***

(1) Amendments to an Alternative Security Program approved under this section may be initiated by—

(i) The submitter of an Alternative Security Program under paragraph (c) of this section; or

(ii) The Coast Guard upon a determination that an amendment is needed to maintain the security of a vessel or facility. The Coast Guard will give the submitter of an Alternative Security Program written notice and request that the submitter propose amendments addressing any matters specified in the notice. The submitter will have at least 60 days to submit its proposed amendments.

(2) Proposed amendments must be sent to the Commandant (CG-5P). If initiated by the submitter, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the Commandant (CG-5P) allows a shorter period. The Commandant (CG-5P) will approve or disapprove the proposed amendment in accordance with paragraph (f) of this section.

(e) ***Validity of Alternative Security Program.*** An Alternative Security Program approved under this section is valid for 5 years from the date of its approval.

(f) The Commandant (CG-5P) will examine each submission for compliance with this part, and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60471, Oct. 22, 2003; USCG-2013-0397, 78 FR 39173, July 1, 2013]

§ 101.125 [Reserved]

§ 101.130 Equivalent security measures.

(a) For any measure required by part 104, 105, or 106 of this subchapter, the owner or operator may substitute an equivalent security measure that has been approved by the Commandant (CG-5P) as meeting or exceeding the effectiveness of the required measure. The Commandant (CG-5P) may require that the owner or operator provide data for use in assessing the effectiveness of the proposed equivalent security measure.

(b) Requests for approval of equivalent security measures should be made to the appropriate plan approval authority under parts 104, 105 or 106 of this subchapter.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended by USCG-2013-0397, 78 FR 39173, July 1, 2013]

Subpart B—Maritime Security (MARSEC) Levels

§ 101.200 MARSEC Levels.

(a) MARSEC Levels advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. Ports, under direction of the local COTP, will respond to changes in the MARSEC Level by implementing the measures specified in the AMS Plan. Similarly, vessels and facilities required to have security plans under part 104, 105, or 106 of this subchapter shall implement the measures specified in their security plans for the applicable MARSEC Level.

(b) Unless otherwise directed, each port, vessel, and facility shall operate at MARSEC Level 1.

(c) The Commandant will set (raise or lower) the MARSEC Level commensurate with risk, and in consideration of any maritime nexus to any active National Terrorism Advisory System (NTAS) alerts. Notwithstanding the NTAS, the Commandant retains discretion to adjust the MARSEC Level when necessary to address any particular security concerns or circumstances related to the maritime elements of the national transportation system.

(d) The COTP may raise the MARSEC Level for the port, a specific marine operation within the port, or a specific industry within the port, when necessary to address an exigent circumstance immediately affecting the security of the maritime elements of the transportation in his/her area of responsibility. Application of this delegated authority will be pursuant to policies and procedures specified by the Commandant.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended by USCG-2013-0397, 78 FR 39173, July 1, 2013]

§ 101.205 [Reserved]

Subpart C—Communication (Port—Facility—Vessel)

§ 101.300 Preparedness communications.

(a) ***Notification of MARSEC Level change.*** The COTP will communicate any changes in the MARSEC Levels through a local Broadcast Notice to Mariners, an electronic means, if available, or as detailed in the AMS Plan.

(b) ***Communication of threats.*** When the COTP is made aware of a threat that may cause a transportation security incident, the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her AOR the following details:

(1) Geographic area potentially impacted by the probable threat;

(2) Any appropriate information identifying potential targets;

(3) Onset and expected duration of probable threat;

(4) Type of probable threat; and

(5) Required actions to minimize risk.

(c) ***Attainment.***

(1) Each owner or operator of a vessel or facility required to have a security plan under parts 104 or 105 of this subchapter affected by a change in the MARSEC Level must ensure confirmation to their local COTP the attainment of measures or actions described in their security plan and any other requirements imposed by the COTP that correspond with the MARSEC Level being imposed by the change.

(2) Each owner or operator of a facility required to have a security plan under part 106 of this subchapter affected by a change in the MARSEC Level must ensure confirmation to their cognizant District Commander the attainment of measures or actions described in their security plan and any other requirements imposed by the District Commander or COTP that correspond with the MARSEC Level being imposed by the change.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

§ 101.305 Reporting.

(a) ***Notification of suspicious activities.*** An owner or operator required to have a security plan under part 104, 105, or 106 of this subchapter shall, without delay, report activities that may result in a transportation security incident to the National Response Center at the following toll free telephone: 1-800-424-8802, direct telephone 202-267-2675, or TDD 202-267-4477. Any other person or entity is also encouraged to report activities that may result in a transportation security incident to the National Response Center.

(b) ***Notification of breaches of security.*** An owner or operator required to have a security plan under parts 104, 105, or 106 of this subchapter shall, without delay, report breaches of security to the National Response Center via one of the means listed in paragraph (a) of this section.

(c) ***Notification of transportation security incident (TSI).***

(1) Any owner or operator required to have a security plan under part 104 or 105 of this subchapter shall, without delay, report a TSI to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(2) Any owner or operator required to have a security plan under part 106 of this subchapter shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(d) Callers to the National Response Center should be prepared to provide as much of the following information as possible:

(1) Their own name and contact information;

(2) The name and contact information of the suspicious or responsible party;

(3) The location of the incident, as specifically as possible; and

(4) The description of the incident or activity involved.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended by USCG-2004-18057, 69 FR 34925, June 23, 2004; USCG-2005-21531, 70 FR 36349, June 23, 2005; USCG-2006-25150, 71 FR 39208, July 12, 2006; USCG-2008-0179, 73 FR 35009, June 19, 2008]

§ 101.310 Additional communication devices.

(a) ***Alert Systems.*** Alert systems, such as the ship security alert system required in SOLAS Chapter XI-2, Regulation 6 (Incorporated by reference, see § 101.115), may be used to augment communication and may be one of the communication methods listed in a vessel or facility security plan under part 104, 105, or 106 of this subchapter.

(b) ***Automated Identification Systems (AIS).*** AIS may be used to augment communication, and may be one of the communication methods listed in a vessel security plan under part 104 of this subchapter. See 33 CFR part 164 for additional information on AIS device requirements.

Subpart D—Control Measures for Security

§ 101.400 Enforcement.

(a) The rules and regulations in this subchapter are enforced by the COTP under the supervision and general direction of the District Commander, Area Commander, and the Commandant. All authority and power vested in the COTP by the rules and regulations in this subchapter is also vested in, and may be exercised by, the District Commander, Area Commander, and the Commandant.

(b) The COTP, District Commander, Area Commander, or Commandant may assign the enforcement authority described in paragraph (a) of this section to any other officer or petty officer of the Coast Guard or other designees authorized by the Commandant.

(c) The provisions in this subchapter do not limit the powers conferred upon Coast Guard commissioned, warrant, or petty officers by any other law or regulation, including but not limited to 33 CFR parts 6, 160, and 165.

§ 101.405 Maritime Security (MARSEC) Directives.

(a)

(1) When the Coast Guard determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against the maritime elements of the national transportation system, the Coast Guard may issue a MARSEC Directive setting forth mandatory measures. Only the Commandant or his/her delegee may issue MARSEC Directives under this section. Prior to issuing a MARSEC Directive, the Commandant or his/her delegee will consult with those Federal agencies having an interest in the subject matter of that MARSEC Directive. All MARSEC Directives issued under this section shall be marked as sensitive security information (SSI) in accordance with 49 CFR part 1520.

(2) When a MARSEC Directive is issued, the Coast Guard will immediately publish a notice in the FEDERAL REGISTER, and affected owners and operators will need to go to their local COTP or cognizant District Commander to acquire a copy of the MARSEC Directive. COTPs and District Commanders will require owners or operators to prove that they are a person required by 49 CFR 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 CFR 1520.5(b), they have a need to know sensitive security information.

(b) Each owner or operator of a vessel or facility to whom a MARSEC Directive applies is required to comply with the relevant instructions contained in a MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

(c) Each owner or operator of a vessel or facility required to have a security plan under parts 104, 105 or 106 of this subchapter that receives a MARSEC Directive must:

(1) Within the time prescribed in the MARSEC Directive, acknowledge receipt of the MARSEC Directive to their local COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander; and

(2) Within the time prescribed in the MARSEC Directive, specify the method by which the measures in the MARSEC Directive have been implemented (or will be implemented, if the MARSEC Directive is not yet effective).

(d) In the event that the owner or operator of a vessel or facility required to have a security plan under part 104, 105, or 106 of this subchapter is unable to implement the measures in the MARSEC Directive, the owner or operator must submit proposed equivalent security measures and the basis for submitting the equivalent security measures to the COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander, for approval.

(e) The owner or operator must submit the proposed equivalent security measures within the time prescribed in the MARSEC Directive. The owner or operator must implement any equivalent security measures approved by the COTP, or, if a facility regulated under part 106 of this subchapter, by their cognizant District Commander.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

§ 101.410 Control and Compliance Measures.

(a) The COTP may exercise authority pursuant to 33 CFR parts 6, 160 and 165, as appropriate, to rectify non-compliance with this subchapter. COTPs or their designees are the officers duly authorized to exercise control and compliance measures under SOLAS Chapter XI-2, Regulation 9, and the ISPS Code (Incorporated by reference, see § 101.115).

(b) Control and compliance measures for vessels not in compliance with this subchapter may include, but are not limited to, one or more of the following:

(1) Inspection of the vessel;

(2) Delay of the vessel;

(3) Detention of the vessel;

(4) Restriction of vessel operations;

(5) Denial of port entry;

(6) Expulsion from port;

(7) Lesser administrative and corrective measures; or

(8) Suspension or revocation of a security plan approved by the U.S., thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(c) Control and compliance measures for facilities not in compliance with this subchapter may include, but are not limited to, one or more of the following:

(1) Restrictions on facility access;

(2) Conditions on facility operations;

(3) Suspension of facility operations;

(4) Lesser administrative and corrective measures; or

(5) Suspension or revocation of security plan approval, thereby making that facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(d) Control and compliance measures under this section may be imposed on a vessel when it has called on a facility or at a port that does not maintain adequate security measures to ensure that the level of security to be achieved by this subchapter has not been compromised.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

§ 101.415 Penalties.

(a) ***Civil and criminal penalty.*** Violation of any order or other requirement imposed under section 101.405 of this part is punishable by the civil and criminal penalties prescribed in 46 U.S.C. 70036 or 46 U.S.C. 70052, as appropriate.

(b) ***Civil penalty.*** As provided in 46 U.S.C. 70119, any person who does not comply with any other applicable requirement under this subchapter, including a Maritime Security Directive, shall be liable to the U.S. for a civil penalty of not more than $ 25,000 for each violation. Enforcement and administration of this provision will be in accordance with 33 CFR 1.07.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended by USCG-2008-0179, 73 FR 35009, June 19, 2008; USCG-2020-0304, 85 FR 58277, Sept. 18, 2020]

§ 101.420 Right to appeal.

(a) Any person directly affected by a decision or action taken by a COTP under this subchapter, may appeal that action or decision to the cognizant District Commander according to the procedures in 46 CFR 1.03-15.

(b) Any person directly affected by a decision or action taken by a District Commander, whether made under this subchapter generally or pursuant to paragraph (a) of this section, with the exception of those decisions made under § 101.410 of this subpart, may appeal that decision or action to the Commandant (CG-5P), according to the procedures in 46 CFR 1.03-15. Appeals of District Commander decisions or actions made under § 101.410 of this subpart should be made to the Commandant (CG-CVC), according to the procedures in 46 CFR 1.03-15.

(c) Any person directly affected by a decision or action taken by the Commanding Officer, Marine Safety Center, under this subchapter, may appeal that action or decision to the Commandant (CG-5P) according to the procedures in 46 CFR 1.03-15.

(d) Decisions made by Commandant (CG-5P), whether made under this subchapter generally or pursuant to the appeal provisions of this section, are considered final agency action.

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003; 68 FR 62502, Nov. 4, 2003; USCG-2008-0179, 73 FR 35009, June 19, 2008; USCG-2013-0397, 78 FR 39173, July 1, 2013]

Subpart E—Other Provisions

§ 101.500 Procedures for authorizing a Recognized Security Organization (RSO). [Reserved]

§ 101.505 Declaration of Security (DoS).

(a) The purpose of a DoS, as described in SOLAS Chapter XI-2, Regulation 10, and the ISPS Code (Incorporated by reference, see § 101.115), is to state the agreement reached between a vessel and a facility, or between vessels in the case of a vessel-to-vessel activity, as to the respective security measures each must undertake during a specific vessel-to-facility interface, during a series of interfaces between the vessel and the facility, or during a vessel-to-vessel activity.

(b) Details as to who must complete a DoS, when a DoS must be completed, and how long a DoS must be retained are included in parts 104 through 106 of this subchapter. A DoS must, at a minimum, include the information found in the ISPS Code, part B, appendix 1 (Incorporated by reference, see § 101.115).

(c) All vessels and facilities required to comply with parts 104, 105, and 106 of this subchapter must, at a minimum, comply with the DoS requirements of the MARSEC Level set for the port.

(d) The COTP may also require a DoS be completed for vessels and facilities during periods of critical port operations, special marine events, or when vessels give notification of a higher MARSEC Level than that set in the COTP's Area of Responsibility (AOR).

[USCG-2003-14792, 68 FR 39278, July 1, 2003, as amended at 68 FR 60472, Oct. 22, 2003]

§ 101.510 Assessment tools.

Ports, vessels, and facilities required to conduct security assessments by part 103, 104, 105, or 106 of this subchapter may use any assessment tool that meets the standards set out in part 103, 104, 105, or 106, as applicable. These tools may include USCG assessment tools, which are available from the cognizant COTP or at *https://www.dco.uscg.mil/Our-Organization/NVIC/*, as set out in the following:

(a) Navigation and Vessel Inspection Circular titled, “Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports” (NVIC 9-02 series);

(b) Navigation and Vessel Inspection Circular titled, “Security Guidelines for Vessels”, (NVIC 10-02 change 1); and

(c) Navigation and Vessel Inspection Circular titled, “Security Guidelines for Facilities”, (NVIC 11-02 change 1).

[USCG-2012-0306, 77 FR 37313, June 21, 2012, as amended by USCG-2013-0397, 78 FR 39173, July 1, 2013; USCG-2022-0323, 88 FR 10028, Feb. 16, 2023]

§ 101.514 TWIC Requirement.

(a) All persons requiring unescorted access to secure areas of vessels, facilities, and OCS facilities regulated by parts 104, 105 or 106 of this subchapter must possess a TWIC before such access is granted, except as otherwise noted in this section. A TWIC must be obtained via the procedures established by TSA in 49 CFR part 1572.

(b) Federal officials are not required to obtain or possess a TWIC. Except in cases of emergencies or other exigent circumstances, in order to gain unescorted access to a secure area of a vessel, facility, or OCS facility regulated by parts 104, 105 or 106 of this subchapter, a Federal official must present his/her agency issued, HSPD 12 compliant credential. Until each agency issues its HSPD 12 compliant cards,

Federal officials may gain unescorted access by using their agency's official credential. The COTP will advise facilities and vessels within his or her area of responsibility as agencies come into compliance with HSPD 12.

(c) Law enforcement officials at the State or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas. They may, however, voluntarily obtain a TWIC where their offices fall within or where they require frequent unescorted access to a secure area of a vessel, facility or OCS facility.

(d) Emergency responders at the State or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas during an emergency situation. They may, however, voluntarily obtain a TWIC where their offices fall within or where they desire frequent unescorted access to a secure area of a vessel, facility or OCS facility in non-emergency situations.

[USCG-2006-24196, 72 FR 3578, Jan. 25, 2007, as amended at 73 FR 25565, May 7, 2008; USCG-2015-0433, 80 FR 44281, July 27, 2015; USCG-2007-28915, 81 FR 57708, Aug. 23, 2016]

§ 101.515 TWIC/Personal Identification.

(a) Persons not described in § 101.514 must present personal identification in order to gain entry to a vessel, facility, and OCS facility regulated by parts 104, 105 or 106 of this subchapter. These individuals must be under escort, as that term is defined in § 101.105 of this part, while inside a secure area. This personal identification must, at a minimum, meet the following requirements:

(1) Be laminated or otherwise secure against tampering;

(2) Contain the individual's full name (full first and last names, middle initial is acceptable);

(3) Contain a photo that accurately depicts that individual's current facial appearance; and

(4) Bear the name of the issuing authority.

(b) The issuing authority in paragraph (a)(4) of this section must be:

(1) A government authority, or an organization authorized to act on behalf of a government authority; or

(2) The individual's employer, union, or trade association.

(c) Vessel, facility, and OCS facility owners and operators must permit law enforcement officials, in the performance of their official duties, who present proper identification in accordance with this section and § 101.514 to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel, facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.

(d) ***Inspection of credential.***

(1) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(2) Each person who has been issued or possesses a TWIC must pass an electronic TWIC inspection, and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a Personal Identification Number, upon a request from TSA, the Coast Guard, any other authorized DHS representative, or a Federal, State, or local law enforcement officer.

[USCG-2006-24196, 72 FR 3578, Jan. 25, 2007, as amended by USCG-2007-28915, 81 FR 57708, Aug. 23, 2016]

§ 101.520 Electronic TWIC inspection.

To conduct electronic TWIC inspection, the owner or operator of a vessel or facility must ensure the following actions are performed.

(a) ***Card authentication.*** The TWIC must be authenticated by performing a challenge/response protocol using the Certificate for Card Authentication (CCA) and the associated card authentication private key stored in the TWIC.

(b) ***Card validity check.*** The TWIC must be checked to ensure the TWIC has not expired and against TSA's list of cancelled TWICs, and no match on the list may be found.

(c) ***Identity verification.***

(1) One of the biometric templates stored in the TWIC must be matched to the TWIC-holder's live sample biometric or, by matching to the PACS enrolled reference biometrics linked to the FASC-N of the TWIC; or

(2) If an individual is unable to provide a valid live sample biometric, the TWIC-holder must enter a Personal Identification Number (PIN) and pass a visual TWIC inspection.

[USCG-2007-28915, 81 FR 57708, Aug. 23, 2016]

§ 101.525 TSA list of cancelled TWICs.

(a) At Maritime Security (MARSEC) Level 1, the card validity check must be conducted using information from the TSA that is no more than 7 days old.

(b) At MARSEC Level 2, the card validity check must be conducted using information from the TSA that is no more than 1 day old.

(c) At MARSEC Level 3, the card validity check must be conducted using information from the TSA that is no more than 1 day old.

(d) The list of cancelled TWICs used to conduct the card validity check must be updated within 12 hours of any increase in MARSEC level, no matter when the information was last updated.

(e) Only the most recently obtained list of cancelled TWICs must be used to conduct card validity checks.

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

§ 101.530 PACS requirements for Risk Group A.

This section lays out requirements for a Physical Access Control System (PACS) that may be used to meet electronic TWIC inspection requirements.

(a) A PACS may use a TWIC directly to perform electronic TWIC inspection;

(b) Each PACS card issued to an individual must be linked to that individual's TWIC, and the PACS must contain the following information from each linked TWIC:

(1) The name of the TWIC-holder holder as represented in the Printed Information container of the TWIC.

(2) The TWIC-signed CHUID (with digital signature and expiration date).

(3) The TWIC resident biometric template.

(4) The TWIC digital facial image.

(5) The PACS Personal Identification Number (PIN).

(c) When first linked, a one-time electronic TWIC inspection must be performed, and the TWIC must be verified as authentic, valid, and biometrically matched to the individual presenting the TWIC.

(d) Each time the PACS card is used to gain access to a secure area, the PACS must—

(1) Conduct identity verification by:

(i) Conducting a biometric scan, and match the result with the biometric template stored in the PACS that is linked to the TWIC, or

(ii) Having the individual enter a stored PACS PIN and conducting a Non-TWIC visual identity verification as defined in § 101.105.

(2) Conduct a card validity check; and

(3) Maintain records in accordance with § 104.235(g) or § 105.225(g) of this subchapter, as appropriate.

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

§ 101.535 Electronic TWIC inspection requirements for Risk Group A.

Owners or operators of vessels or facilities subject to part 104 or 105 of this subchapter, that are assigned to Risk Group A in § 104.263 or § 105.253 of this subchapter, must ensure that a Transportation Worker Identification Credential (TWIC) Program is implemented as follows:

(a) ***Requirements for Risk Group A vessels.*** Prior to each boarding of the vessel, all persons who require access to a secure area of the vessel must pass an electronic TWIC inspection before being granted unescorted access to the vessel.

(b) ***Requirements for Risk Group A facilities.*** Prior to each entry into a secure area of the facility, all persons must pass an electronic TWIC inspection before being granted unescorted access to secure areas of the facility.

(c) A Physical Access Control System that meets the requirements of § 101.530 may be used to meet the requirements of this section.

(d) The requirements of this section do not apply under certain situations described in § 101.550 or § 101.555.

(e) Emergency access to secure areas, including access by law enforcement and emergency responders, does not require electronic TWIC inspection.

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

§ 101.540 Electronic TWIC inspection requirements for vessels, facilities, and OCS facilities not in Risk Group A.

A vessel or facility not in Risk Group A may use the electronic TWIC inspection requirements of § 101.535 in lieu of visual TWIC inspection. If electronic TWIC inspection is used, the recordkeeping requirements of § 104.235(b)(9) and (c) of this subchapter, or § 105.225(b)(9) and (c) of this subchapter, as appropriate, apply.

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

§ 101.545 [Reserved]

§ 101.550 TWIC inspection requirements in special circumstances.

Owners or operators of any vessel, facility, or Outer Continental Shelf (OCS) facility subject to part 104, 105, or 106 of this subchapter must ensure that a Transportation Worker Identification Credential (TWIC) Program is implemented as follows:

(a) ***Lost, damaged, stolen, or expired TWIC.*** If an individual cannot present a TWIC because it has been lost, damaged, stolen, or expired, and the individual previously has been granted unescorted access to secure areas and is known to have had a TWIC, the individual may be granted unescorted access to secure areas for a period of no longer than 30 consecutive calendar days if—

(1) The individual provides proof that he or she has reported the TWIC as lost, damaged, or stolen to the Transportation Security Administration (TSA) as required in 49 CFR 1572.19(f), or the individual provides proof that he or she has applied for the renewal of an expired TWIC;

(2) The individual can present another identification credential that meets the requirements of § 101.515; and

(3) There are no other suspicious circumstances associated with the individual's claim that the TWIC was lost, damaged, or stolen.

(b) ***TWIC on the Canceled Card List.*** In the event an individual reports his or her TWIC as lost, damaged, or stolen, and that TWIC is then placed on the Canceled Card List, the individual may be granted unescorted access by a Physical Access Control System (PACS) that meets the requirements of § 101.530 for a period of no longer than 30 days. The individual must be known to have had a TWIC, and known to have reported the TWIC as lost, damaged, or stolen to TSA.

(c) ***Special requirements for Risk Group A vessels and facilities.*** If a TWIC reader or a PACS cannot read an individual's biometric templates due to poor biometric quality or no biometrics enrolled, the owner or operator may grant the individual unescorted access to secure areas based on either of the following secondary authentication procedures:

(1) The owner or operator must conduct a visual TWIC inspection and require the individual to correctly submit his or her TWIC Personal Identification Number.

(2) [Reserved]

(d) If an individual cannot present a TWIC for any reason other than those outlined in paragraphs (a) or (b) of this section, the vessel or facility operator may not grant the individual unescorted access to secure areas. The individual must be under escort at all times while in the secure area.

(e) With the exception of individuals granted access according to paragraphs (a) or (b) of this section, all individuals granted unescorted access to secure areas of a vessel, facility, or OCS facility must be able to produce their TWICs upon request from the TSA, the 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]