SUBCHAPTER H—MARITIME SECURITY

PART 101—MARITIME SECURITY: GENERAL

Subpart A—General

Subpart B—Maritime Security (MARSEC) Levels

Subpart C—Communication (Port-Facility-Vessel)

Subpart D—Control Measures for Security

Subpart E—Other Provisions

Subpart F—Cybersecurity

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.

EFFECTIVE DATE NOTE: By USCG–2022–0802, 90 FR 6447, Jan. 17, 2025, the part 101 authority citation was amended, effective July 16, 2025.

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 reboarding 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 record-keeping 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]

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.

§ 101.615 Definitions.

Unless otherwise specified, as used in this subpart:

Approved list means an owner or operator's authoritative catalog for products that meet cybersecurity requirements.

Backup means a copy of physical or virtual files or databases stored separately for preservation and recovery. It may also refer to the process of creating a copy.

Credentials means a set of data attributes that uniquely identifies a system entity such as a person, an organization, a service, or a device, and attests to one's right to access to a particular system.

Critical Information Technology (IT) or Operational Technology (OT) systems means any Information Technology (IT) or Operational Technology (OT) system used by the vessel, facility, or OCS facility that, if compromised or exploited, could result in a transportation security incident (TSI), as determined by the Cybersecurity Officer (CySO) in the Cybersecurity Plan. Critical IT or OT systems include those business support services that, if compromised or exploited, could result in a TSI. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system, or actually jeopardizes, without lawful authority, an information system.

Cyber Incident Response Plan means a set of predetermined and documented procedures to respond to a cyber incident. It is a document that gives the owner or operator or a designated CySO instructions on how to respond to a cyber incident and pre-identifies key roles, responsibilities, and decision-makers.

Cyber threat means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term ''cyber threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity Assessment means the appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes identification of relevant vulnerabilities and threats and determining the extent to which adverse circumstances or events could result in operational disruption and other harmful consequences.

Cybersecurity Officer, or CySO, means the person designated as responsible for the development, implementation, and maintenance of the cybersecurity portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security Officers. The owner or operator may designate an alternate CySO(s) to assist with the duties and responsibilities of the CySO, including during periods when the CySO is on leave, unavailable, or unable to perform their duties. Hereafter, ''CySO'' will refer to both the CySO and the alternate CySO(s), as applicable.

Cybersecurity Plan means a plan developed as a part of the VSP, FSP, or OCS FSP to ensure application and implementation of cybersecurity measures designed to protect the owners' or operators' systems and equipment, as required by this part. A Cybersecurity Plan is either included in a VSP, FSP, or OCS FSP; as an annex to a VSP, FSP, or OCS FSP; provided in a separate submission from the VSP, FSP, or OCS FSP; or addressed through an Alternative Security Program.

Cybersecurity risk means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism. It does not include any action that solely involves a

violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity vulnerability means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Encryption means any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

Executable code means any object code, machine code, or other code readable by a computer when loaded into its memory and used directly by such computer to execute instructions.

Exploitable channel means any information channel (such as a portable media device and other hardware) that allows for the violation of the security policy governing the information system and is usable or detectable by subjects external to the trusted user.

Firmware means computer programs (which are stored in and executed by computer hardware) and associated data (which is also stored in the hardware) that may be dynamically written or modified during execution.

Hardware means, collectively, the equipment that makes up physical parts of a computer, including its electronic circuitry, together with keyboards, readers, scanners, and printers.

Human-Machine Interface, or HMI, means the hardware or software through which an operator interacts with a controller for industrial systems. An HMI can range from a physical control panel with buttons and indicator lights to an industrial personal computer with a color graphics display running dedicated HMI software.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software data, applications, communications, and people. It includes the application of IT, OT, or a combination of both.

Information Technology, or IT, means any equipment or interconnected system or subsystem of equipment, used in the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Known Exploited Vulnerability, or KEV, means a computer vulnerability that has been exploited in the past.

Log means a record of the events occurring within an organization's systems and networks.

Multifactor authentication means a layered approach to securing data and applications for a system that requires users to present more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Network means information system(s) implemented with a collection of interconnected components. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. A network consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications.

Network map means a visual representation of internal network topologies and components.

Network segmentation means a physical or virtual architectural approach that divides a network into multiple segments, each acting as its own subnetwork, to provide additional security and control that can help prevent or minimize the impact of a cyber incident.

Operational Technology, or OT, means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a change through the monitoring or control of devices, processes, and events.

Patching means updating software and operating systems to address cybersecurity vulnerabilities within a program or product.

Penetration test means a test of the security of a computer system or software application by attempting to

compromise its security and the security of an underlying operating system and network component configurations.

Principle of least privilege means that an individual should be given only those privileges that are needed to complete a task. Further, the individual's function, not identity, should control the assignment of privileges.

Privileged user means a user who is authorized (and, therefore, trusted) to perform security functions that ordinary users are not authorized to perform.

Reportable cyber incident means an incident that leads to or, if still under investigation, could reasonably lead to any of the following: Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system; Disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; Disclosure or unauthorized access directly or indirectly of nonpublic personal information of a significant number of individuals; Other potential operational disruption to critical infrastructure systems or assets; or Incidents that otherwise may lead to a transportation security incident as defined in 33 CFR 101.105.

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and the likelihood of occurrence.

Software means a set of instructions, data, or programs used to operate a computer and execute specific tasks.

Supply chain means a system of organizations, people, activities, information, and resources for creating computer products and offering IT services to their customers.

Threat means any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system through unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerability means a characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Vulnerability scan means a technique used to identify hosts or host attributes and associated vulnerabilities.

§ 101.620 Owner or operator.

(a) Each owner or operator of a U.S.-flagged vessel, facility, or OCS facility is responsible for compliance with the requirements of this subpart.

(b) For each U.S.-flagged vessel, facility, or OCS facility, the owner or operator must—

(1) Ensure a Cybersecurity Plan is developed, approved, and maintained;

(2) Define in Section 1 of the Cybersecurity Plan the cybersecurity organizational structure and identify each person exercising cybersecurity duties and responsibilities within that structure, with the support needed to fulfill those obligations;

(3) Designate, in writing, by name and by title, a Cybersecurity Officer (CySO) who is accessible to the Coast Guard 24 hours a day, 7 days a week, and identify how the CySO can be contacted at any time;

(4) Ensure that cybersecurity exercises, audits, and inspections, as well as the Cybersecurity Assessment, are conducted as required by this part and in accordance with the Cybersecurity Plan (see § 101.625(d)(1), (3), (6) and (7));

(5) Ensure that the U.S.-flagged vessel, facility, or OCS facility operates in compliance with the approved Cybersecurity Plan;

(6) Ensure the development, approval, and execution of the Cyber Incident Response Plan; and

(7) For entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16–1, ensure all reportable cyber incidents are reported to the National Response Center (NRC).

§ 101.625 Cybersecurity Officer.

(a) *Other duties.* The Cybersecurity Officer (CySO) may serve in other roles or positions and may perform other duties within the owner's or operator's organization (U.S.-flagged vessel, facility, or OCS facility), provided the person is able to perform the duties and responsibilities required of the CySO by this part.

(b) *Serving as CySO for Multiple Vessels, Facilities, or OCS Facilities.* The same person may serve as the CySO for more than one U.S.-flagged vessel, facility, or OCS facility. If a person serves as the CySO for more than one U.S.-flagged vessel, facility, or OCS facility, the name of each U.S.-flagged vessel, facility, or OCS facility for which that person is the CySO must be listed in the Cybersecurity Plan of each U.S.-flagged vessel, facility, or OCS facility for which that person is the CySO.

(c) *Assigning Duties Permitted.* The CySO may assign security duties to other U.S.-flagged vessel, facility, or OCS facility personnel; however, the CySO retains ultimate responsibility for these duties.

(d) *Responsibilities.* For each U.S.-flagged vessel, facility, or OCS facility for which they are designated, the CySO must—

(1) Ensure that the Cybersecurity Assessment is conducted as required by this part;

(2) Ensure the cybersecurity measures in the Cybersecurity Plan are developed, implemented, and operating as intended;

(3) Ensure that an annual audit of the Cybersecurity Plan and its implementation is conducted and, if necessary, ensure that the Cybersecurity Plan is updated;

(4) Ensure the Cyber Incident Response Plan is executed and exercised;

(5) Ensure the Cybersecurity Plan is exercised in accordance with § 101.635(c);

(6) Arrange for cybersecurity inspections, which may be conducted as their own inspections, or in conjunction with any scheduled Coast Guard inspection of a U.S.-flagged vessel, facility, or OCS facility;

(7) Ensure the prompt correction of problems identified by exercises, audits, or inspections;

(8) Enhance the cybersecurity awareness and vigilance of personnel;

(9) Ensure adequate cybersecurity training of personnel;

(10) Ensure all reportable cyber incidents are recorded and reported to the owner or operator;

(11) Ensure that records required by this part are maintained in accordance with § 101.640;

(12) Ensure any reports as required by this part have been prepared and submitted;

(13) Ensure that the Cybersecurity Plan, as well as proposed amendments to cybersecurity measures included in the Plan, are submitted for approval to the cognizant COTP or the Officer in Charge, Marine Inspections (OCMI) for facilities or OCS facilities, or to the Marine Safety Center (MSC) for U.S.-flagged vessels, prior to amending the Cybersecurity Plan, in accordance with § 101.630;

(14) Ensure relevant security and management personnel are briefed regarding changes in cybersecurity conditions on board the U.S.-flagged vessel, facility, or OCS facility; and

(15) Ensure identification and mitigation of all KEVs in critical IT or OT systems, without delay.

(e) *Qualifications.* The CySO must have general knowledge, through training, education, or equivalent job experience, in the following:

(1) General vessel, facility, or OCS facility operations and conditions;

(2) General cybersecurity guidance and best practices;

(3) The vessel, facility, or OCS facility's Cyber Incident Response Plan;

(4) The vessel, facility, or OCS facility's Cybersecurity Plan;

(5) Cybersecurity equipment and systems;

(6) Methods of conducting cybersecurity audits, inspections, control, and monitoring techniques;

(7) Relevant laws and regulations pertaining to cybersecurity;

(8) Instruction techniques for cybersecurity training and education;

(9) Handling of Sensitive Security Information and security related communications;

(10) Current cybersecurity threat patterns and KEVs;

(11) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security; and

(12) Conducting and assessing cybersecurity drills and exercises.

§ 101.630 Cybersecurity Plan.

(a) *General.* The CySO must develop, implement, and verify a Cybersecurity Plan for U.S.-flagged vessels, facilities, or OCS facilities. The Cybersecurity Plan must reflect all cybersecurity measures required in this subpart, as appropriate, to mitigate risks identified during the Cybersecurity Assessment. The Plan must describe in detail how the requirements of subpart F will be met. The Cybersecurity Plan may be included in a VSP, FSP, or an OCS FSP; as an annex to the VSP, FSP, or OCS FSP; as part of an approved Alternative Security Program; or may be provided in a separate submission from the VSP, FSP, or OCS FSP.

(b) *Protecting sensitive security information.* The Cybersecurity Plan is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(c) *Format.* The owner or operator must ensure that the Cybersecurity Plan consists of the individual sections listed in this paragraph. If the Cybersecurity Plan does not follow the order as it appears on the list, the owner or operator must ensure that the Plan contains an index identifying the location of each of the following sections:

(1) Cybersecurity organization and identity of the CySO;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Communications;

(6) Cybersecurity systems and equipment, with associated maintenance;

(7) Cybersecurity measures for access control, including the computer, IT, and OT access areas;

(8) Physical security controls for IT and OT systems;

(9) Cybersecurity measures for monitoring;

(10) Audits and amendments to the Cybersecurity Plan;

(11) Reports of all cybersecurity audits and inspections, to include documentation of resolution or mitigation of all identified vulnerabilities;

(12) Documentation of all identified, unresolved vulnerabilities, to include those that are intentionally unresolved due to owner or operator risk acceptance;

(13) Cyber incident reporting procedures in accordance with part 101 of this subchapter; and

(14) Cybersecurity Assessment.

(d) *Submission and approval.* Each owner or operator must submit one copy of their Cybersecurity Plan for review and approval to the cognizant COTP or the OCMI for a facility or OCS facility, or to the MSC for a U.S.-flagged vessel.

(1) The COTP, OCMI, or MSC will evaluate each submission for compliance with this part, and either—

(i) Approve the Cybersecurity Plan and return a letter to the owner or operator indicating approval and any conditional approval;

(ii) Require additional information or revisions to the Cybersecurity Plan and return a copy to the owner or operator with a brief description of the required revisions or additional information; or

(iii) Disapprove the Cybersecurity Plan and return a copy to the owner or operator with a brief statement of the reasons for disapproval.

(iv) If the cognizant COTP, OCMI, or MSC requires additional time to review the Plan, they may return a written acknowledgement to the owner or operator stating that the Coast Guard will review the Cybersecurity Plan submitted for approval, and that the U.S.-flagged vessel, facility, or OCS facility may continue to operate as long as it remains in compliance with the submitted Cybersecurity Plan.

(2) Owners or operators submitting one Cybersecurity Plan to cover two or more U.S.-flagged vessels, facilities, or OCS facilities of similar operations must ensure the Plan addresses the specific cybersecurity risks for each U.S.-flagged vessel, facility, or OCS facility.

(3) A Plan that is approved by the COTP, OCMI, or MSC is valid for 5 years from the date of its approval.

(e) *Amendments to the Cybersecurity Plan.* (1) Amendments to a Coast

Guard-approved Cybersecurity Plan must be initiated by either—

(i) The owner or operator or the CySO; or

(ii) When the COTP, OCMI, or MSC finds that the Cybersecurity Plan no longer meets the requirements in this part, the Plan will be returned to the owner or operator with a letter explaining why the Plan no longer meets the requirements and requires amendment. The owner or operator will have at least 60 days to submit its proposed amendments. Until the amendments are approved, the owner or operator must ensure temporary cybersecurity measures are implemented to the satisfaction of the Coast Guard.

(2) Proposed amendments to the Cybersecurity Plan must be sent to the Coast Guard at least 30 days before the proposed amendment's effective date. The Coast Guard will approve or disapprove the proposed amendment in accordance with this part.

(i) Nothing in this section should be construed as limiting the owner or operator of the U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures not enumerated in the approved VSP, FSP, or OCS FSP as necessary to address exigent security situations.

(ii) In such cases, the owner or operator must notify the cognizant COTP for a facility or OCS facility, or the MSC for U.S.-flagged vessels, by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(3) If the owner or operator has changed, the CySO must amend the Cybersecurity Plan as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours, to include the name and contact information of the new owner or operator and submit the affected portion of the Plan for review and approval in accordance with this part.

(4) If the CySO has changed, the Coast Guard must be notified as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours, and the affected portion of the Cybersecurity Plan must be amended and submitted to the Coast Guard for review and approval in accordance with this part as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours.

(f) *Audits.* (1) The CySO must ensure that an audit of the Cybersecurity Plan and its implementation is performed annually, beginning no later than 1 year from the initial date of approval. The CySO must attach a report to the Plan certifying that the Plan meets the applicable requirements of this subpart.

(2) In addition to the annual audit, the CySO must ensure that an audit of the Cybersecurity Plan occurs if there is a change in the owner or operator of the U.S.-flagged vessel, facility, or OCS facility, or if there have been modifications to the cybersecurity measures, including, but not limited to, physical access, incident response procedures, security measures, or operations.

(3) Additional audits of the Cybersecurity Plan as a result of modifications to the U.S.-flagged vessel, facility, or OCS facility, or because of changes to the cybersecurity measures in accordance with paragraph (f)(2) of this section, may be limited to those sections of the Plan affected by the modifications.

(4) Personnel conducting internal audits of the cybersecurity measures specified in the Plan or evaluating its implementation must—

(i) Have knowledge of methods of conducting audits and inspections, as well as access control and monitoring techniques;

(ii) Not have regularly assigned cybersecurity duties for the U.S.-flagged vessel, facility, or OCS facility being audited; and

(iii) Be independent of any cybersecurity measures being audited.

(5) If the results of an audit require amending the Cybersecurity Plan, the CySO must submit, in accordance with this part, the amendments to the Coast Guard for review and approval no later than 30 days after completion of the audit.

§ 101.635 Drills and exercises.

(a) *General.* (1) Drills and exercises must be used to test the proficiency of the U.S.-flagged vessel, facility, and OCS facility personnel in assigned cybersecurity duties and the effective implementation of the VSP, FSP, OCS FSP, and Cybersecurity Plan. The drills and exercises must enable the CySO to identify any related cybersecurity deficiencies that need to be addressed.

(2) The drill or exercise requirements specified in this section may be satisfied with the implementation of cybersecurity measures required by the VSP, FSP, OCS FSP, and Cybersecurity Plan as the result of a cyber incident, as long as the U.S.-flagged vessel, facility, or OCS facility achieves and documents attainment of drill and exercise goals for the cognizant COTP.

(b) *Drills.* (1) The CySO must ensure that cybersecurity drills are conducted at least twice each calendar year. Cybersecurity drills may be held in conjunction with other security or non-security drills, as required by 33 CFR 104.230, 105.220, or 106.225, where appropriate.

(2) Drills must test individual elements of the Cybersecurity Plan, including responses to cybersecurity threats and incidents. Cybersecurity drills must take into account the types of operations of the U.S.-flagged vessel, facility, or OCS facility; changes to the U.S.-flagged vessel, facility, or OCS facility personnel; the type of vessel a facility is serving; and other relevant circumstances.

(3) If a vessel is moored at a facility on a date a facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be—

(i) Full-scale or live;

(ii) Tabletop simulation;

(iii) Combined with other appropriate exercises as required by 33 CFR 104.230, 105.220, or 106.225; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel-, facility-, or OCS facility-specific, or part of a cooperative exercise program to exercise applicable vessel, facility, and OCS facility Cybersecurity Plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the cybersecurity program and must include the substantial and active participation of the CySO(s).

(6) If any corrective action identified during an exercise is needed, it must be addressed and documented as soon as possible.

§ 101.640 Records and documentation.

All records, reports, and other documents mentioned in this subpart must be created and maintained in accordance with 33 CFR 104.235 for U.S.-flagged vessels, 105.225 for facilities, and 106.230 for OCS facilities. At a minimum, the records must be created for the following activities: training, drills, exercises, cybersecurity threats, reportable cyber incidents, and audits of the Cybersecurity Plan.

§ 101.645 Communications.

(a) The CySO must have a means to effectively notify owners or operators and personnel of a U.S.-flagged vessel, facility, or OCS facility of changes in cybersecurity conditions at the U.S.-flagged vessel, facility, and OCS facility and document these means in Section 5 of the Cybersecurity Plan.

(b) Communication systems and procedures must allow effective and continuous communications between U.S.-flagged vessel, facility, and OCS facility security personnel, vessels interfacing with a facility or an OCS facility, the cognizant COTP, and national and local authorities with security responsibilities.

§ 101.650 Cybersecurity measures.

(a) *Account security measures.* Each owner or operator of a U.S.-flagged vessel, facility, or OCS facility must ensure, at a minimum, the following account security measures are in place and documented in Section 7 of the Cybersecurity Plan:

(1) Automatic account lockout after repeated failed login attempts must be enabled on all password-protected IT systems;

(2) Default passwords must be changed before using any IT or OT systems. When changing default passwords is not feasible, appropriate compensating security controls must be implemented and documented;

(3) A minimum password strength must be maintained on all IT and OT systems that are technically capable of password protection;

(4) Multifactor authentication must be implemented on password-protected IT and remotely accessible OT systems. When multifactor authentication is not feasible, appropriate compensating security controls must be implemented and documented;

(5) The principle of least privilege must be applied to administrator or otherwise privileged accounts on both IT and OT systems;

(6) The owner or operator must ensure that users maintain separate credentials on critical IT and OT systems; and

(7) The owner or operator must ensure that user credentials are removed or revoked when a user leaves the organization.

(b) *Device security measures.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following device security measures are in place, addressed in Section 6 of the Cybersecurity Plan, and made available to the Coast Guard upon request:

(1) Develop and maintain a list of approved hardware, firmware, and software that may be installed on IT or OT systems. Any hardware, firmware, and software installed on IT and OT systems must be on the owner- or operator-approved list;

(2) Ensure applications running executable code are disabled by default on critical IT and OT systems;

(3) Maintain an accurate inventory of network-connected systems, including designation of critical IT and OT systems; and

(4) Develop and maintain accurate documentation identifying the network map and OT device configuration information.

(c) *Data security measures.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following data security measures are in place and documented in Section 4 of the Cybersecurity Plan:

(1) Logs must be securely captured, stored, and protected so that they are accessible only by privileged users; and

(2) Effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible.

(d) *Cybersecurity training for personnel.* The training program to address requirements under this paragraph must be documented in Sections 2 and 4 of the Cybersecurity Plan.

(1) All personnel with access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must have cybersecurity training in the following topics:

(i) Relevant provisions of the Cybersecurity Plan;

(ii) Recognition and detection of cybersecurity threats and all types of cyber incidents;

(iii) Techniques used to circumvent cybersecurity measures;

(iv) Procedures for reporting a cyber incident to the CySO; and

(v) OT-specific cybersecurity training for all personnel whose duties include using OT.

(2) Key personnel with access to the IT or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must also have cybersecurity training in the following additional topics:

(i) Understanding their roles and responsibilities during a cyber incident and response procedure; and

(ii) Maintaining current knowledge of changing cybersecurity threats and countermeasures.

(3) When personnel must access IT or OT systems but are unable to receive cybersecurity training as specified in paragraphs (d)(1) and (2) of this section, they must be accompanied or monitored by a person who has completed the training specified in paragraphs (d)(1) and (2) of this section.

(4) All personnel must complete the training specified in paragraphs (d)(1)(ii) through (v) of this section by January 12, 2026, and annually thereafter. Key personnel must complete the training specified in paragraph (d)(2) of this section by January 12, 2026, and annually thereafter, or more frequently as needed. Training for new personnel not in place at the time of the effective date of this rule must be completed within 5 days of gaining system access, but no later than within 30 days of hiring, and annually thereafter. Training for personnel on new IT or OT systems not in place at the time of the effective date of this rule must be completed within 5 days of system access, and annually thereafter. All personnel must complete the training specified in paragraph (d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan. The training must be documented and maintained in the owner's or operator's records in accordance with 33 CFR 104.235 for U.S.-flagged vessels, 105.225 for facilities, and 106.230 for OCS facilities.

(e) *Risk management.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following measures for risk management are in place and documented in Sections 11 and 12 of the Cybersecurity Plan:

(1) *Cybersecurity Assessment.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure completion of a Cybersecurity Assessment that addresses each covered U.S.-flagged vessel, facility, and OCS facility. A Cybersecurity Assessment must be conducted no later than July 16, 2027, and annually thereafter. However, the Cybersecurity Assessment must be conducted sooner than annually if there is a change in ownership of a U.S.-flagged vessel, facility, or OCS facility. In conducting the Cybersecurity Assessment, the owner or operator must—

(i) Analyze all networks to identify vulnerabilities to critical IT and OT systems and the risk posed by each digital asset;

(ii) Validate the Cybersecurity Plan;

(iii) Document recommendations and resolutions in the Vessel Security Assessment (VSA), Facility Security Assessment (FSA), or OCS FSA, in accordance with 33 CFR 104.305, 105.305, and 106.305;

(iv) Document and ensure patching or implementing of documented compensating controls for all KEVs in critical IT or OT systems, without delay; and

(v) Incorporate recommendations and resolutions from paragraph (e)(1)(iii) of this section into the Cybersecurity Plan through an amendment, in accordance with §101.630(e).

(2) *Penetration testing.* In conjunction with Cybersecurity Plan renewal, the owner, operator, or designated CySO must ensure that a penetration test has been completed. Following the penetration test, a letter certifying that the test was conducted, as well as all identified vulnerabilities, must be included in the VSA, FSA, or OCS FSA, in accordance with 33 CFR 104.305, 105.305, and 106.305.

(3) *Routine system maintenance.* Each owner or operator or a designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following measures for routine system maintenance are in place and documented in Section 6 of the Cybersecurity Plan:

(i) Ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, without delay;

(ii) Maintain a method to receive and act on publicly submitted vulnerabilities;

(iii) Maintain a method to share threat and vulnerability information with external stakeholders;

(iv) Ensure there are no exploitable channels directly exposed to internet-accessible systems;

(v) Ensure no OT is connected to the publicly accessible internet unless explicitly required for operation, and verify that, for any remotely accessible OT system, there is a documented justification; and

(vi) Conduct vulnerability scans as specified in the Cybersecurity Plan.

(f) *Supply chain.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following supply-chain measures are in place and documented in Section 4 of the Cybersecurity Plan:

(1) Consider cybersecurity capability as criteria for evaluation to procure IT and OT systems or services;

(2) Establish a process through which all IT and OT vendors or service providers notify the owner or operator or designated CySO of any cybersecurity vulnerabilities or reportable cyber incidents, without delay; and

(3) Monitor and document all third-party remote connections to detect cyber incidents.

(g) *Resilience.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following measures for resilience are in place and documented in Sections 3 and 9 of the Cybersecurity Plan:

(1) For entities that have not reported to the Coast Guard pursuant to, or not subject to, 33 CFR 6.16–1, report reportable cyber incidents to the NRC without delay;

(2) In addition to other plans mentioned in this subpart, develop, implement, maintain, and exercise the Cyber Incident Response Plan;

(3) Periodically validate the effectiveness of the Cybersecurity Plan through annual exercises, annual reviews of incident response cases, or post-cyber incident review, as determined by the owner or operator; and

(4) Perform backup of critical IT and OT systems, with those backups being sufficiently protected and tested frequently.

(h) *Network segmentation.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following measures for network segmentation are in place and documented in Sections 7 and 8 of the Cybersecurity Plan:

(1) Implement segmentation between IT and OT networks; and

(2) Verify that all connections between IT and OT systems are logged and monitored for suspicious activity, breaches of security, TSIs, unauthorized access, and cyber incidents.

(i) *Physical security.* Each owner, operator, or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the following measures for physical security are in place and documented in Sections 7 and 8 of the Cybersecurity Plan:

(1) In addition to any other requirements in this part, limit physical access to OT and related IT equipment to only authorized personnel, and confirm that all HMIs and other hardware are secured, monitored, and logged for personnel access; and

(2) Ensure unauthorized media and hardware are not connected to IT and OT infrastructure, including blocking, disabling, or removing unused physical access ports, and establishing procedures for granting access on a by-exception basis.

§ 101.655 Cybersecurity compliance dates.

All Cybersecurity Plans mentioned in this subpart must be submitted to the Coast Guard for review and approval no later than July 16, 2027, according to 33 CFR 104.410 for U.S.-flagged vessels, 33 CFR 105.410 for facilities, or 33 CFR 106.410 for OCS facilities.

§ 101.660 Cybersecurity compliance documentation.

Each owner or operator must ensure that the cybersecurity portion of their Plan and penetration test results are available to the Coast Guard upon request. The Alternative Security Program provisions apply to cybersecurity compliance documentation and are addressed in 33 CFR 104.140 for vessels, 33 CFR 105.140 for facilities, and 33 CFR 106.135 for OCS facilities.

§ 101.665 Noncompliance, waivers, and equivalents.

An owner or operator, after completion of the required Cybersecurity Assessment, may seek a waiver or an equivalence determination for the requirements in subpart F using the standards and submission procedures applicable to a U.S.-flagged vessel, facility, or OCS facility as outlined in 33 CFR 101.130, 104.130, 104.135, 105.130, 105.135, 106.125, or 106.130. If an owner or

operator must temporarily deviate from the requirements in this part, they must notify the cognizant COTP for facilities or OCS facilities, or the MSC for U.S.-flagged vessels, and may request temporary permission to continue to operate under the provisions as outlined in 33 CFR 104.125, 105.125, or 106.120.

§ 101.670 Severability.

Any provision of this subpart held to be invalid or unenforceable as applied to any person or circumstance shall be construed so as to continue to give the maximum effect to the provision permitted by law, including as applied to persons not similarly situated or to dissimilar circumstances, unless such holding is that the provision of this subpart is invalid and unenforceable in all circumstances, in which event the provision shall be severable from the remainder of this subpart and shall not affect the remainder thereof.

PART 102—MARITIME SECURITY: NATIONAL MARITIME TRANSPORTATION SECURITY [RESERVED]

PART 103—MARITIME SECURITY: AREA MARITIME SECURITY

Subpart A—General

Sec.

Subpart B—Federal Maritime Security Coordinator (FMSC) Designation and Authorities

Subpart C—Area Maritime Security (AMS) Committee

Subpart D—Area Maritime Security (AMS) Assessment

Subpart E—Area Maritime Security (AMS) Plan

AUTHORITY: 46 U.S.C. 70034, 70051, 70102, 70103, 70104, 70112, 70116; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

SOURCE: USCG–2003–14733, 68 FR 39290, July 1, 2003, unless otherwise noted.

Subpart A—General

§ 103.100 Applicability.

This part applies to all vessels and facilities located in, on, under, or adjacent to waters subject to the jurisdiction of the U.S.

§ 103.105 Definitions.

Except as specifically stated in this subpart, the definitions in part 101 of this subchapter apply to this part.

Subpart B—Federal Maritime Security Coordinator (FMSC) Designation and Authorities

§ 103.200 Designation of the Federal Maritime Security Coordinator (FMSC).

The COTPs are the Federal Maritime Security Coordinators for their respective COTP zones described in 33 CFR part 3, including all ports and areas located therein.

§ 103.205 Authority of the COTP as the Federal Maritime Security Coordinator (FMSC).

(a) Without limitation to the authority vested in the COTP by statute or regulation, and in addition to authority prescribed elsewhere in this part, the COTP as the FMSC is authorized to: