

U.S. Department of
Homeland Security

United States
Coast Guard



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-3PCP
Phone: (202) 372-1092
Fax: (202) 372-1906

COMDTPUB P16XXX.X
NVIC 07-XX

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 07-XX

Subj: GUIDANCE FOR THE IMPLEMENTATION OF THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM IN THE MARITIME SECTOR

- Ref:
- (a) Title 33 of the Code of Federal Regulations (33 CFR) Parts 101-106
 - (b) Title 49 of the Code of Federal Regulations (49 CFR) Part 1515
 - (c) Title 49 of the Code of Federal Regulations (49 CFR) Part 1570
 - (d) Title 49 of the Code of Federal Regulations (49 CFR) Part 1572
 - (e) NVIC 03-03 Change 1 – Implementation of MTSA Regulations for Facilities
 - (f) NVIC 04-03 Change 1 – Verification of Vessel Security Plans for domestic vessels in accordance with MTSA Regulations and ISPS Code
 - (g) NVIC 05-03 Implementation of MTSA Regulations for Outer Continental Shelf Facilities

1. PURPOSE. This Navigation and Inspection Circular (NVIC) provides guidance on implementation of the Final Rule – Transportation Worker Identification Credential Implementation in the Maritime Sector; Hazardous Material Endorsement for a Commercial Driver's License (FR XXXXX) (referred to as the TWIC rule) – which made major changes to 33 CFR Chapter I Subchapter H, 46 CFR Chapter I Subchapter B, and 49 CFR Chapter XII Subchapter D. The Transportation Worker Identification Credential (TWIC) is required by 46 U.S.C. § 70105, the Maritime Transportation Security Act of 2002 (MTSA) with additional requirements in the SAFE Port Act of 2006. The information in this NVIC details the enrollment and issuance process, provides guidance for successful execution of compliance requirements, provides clarification of the regulations found in references (a) through (d), and includes a more detailed discussion of the actions required by those regulations, with examples, to increase understanding and promote nationwide consistency. These guidelines are intended to help industry and the Coast Guard Captains of the Port (COTP) implement the TWIC Program.
2. ACTION.
 - a. The following individuals must obtain a TWIC (as stated in 46 U.S.C. § 70105):
 - 1) All credentialed U.S. Merchant Mariners (this includes all persons holding a Coast Guard-issued merchant mariner's license, merchant mariner's document, or certificate of registry;
 - 2) Anyone allowed unescorted access to secure areas of U.S.-flagged vessels, facilities, and OCS facilities subject to 33 CFR part 104, 105, and 106 respectively (hereafter referred to as vessels and facilities);

- 3) A vessel pilot.¹
 - 4) All individuals working aboard towing vessels that push, pull or haul alongside tank vessels.²
- b. Vessel and facility owners or operators, U.S. merchant mariners, and maritime transportation workers are encouraged to use this circular as guidance for the enrollment and receipt of TWICs
 - c. Vessel and facility owners or operators are also encouraged to use this guidance to assist in ensuring that all requirements in the establishment of a TWIC Program are met including but not limited to: informing personnel of TWIC responsibilities, escorting procedures, and management of access control. This guidance will also assist in preparation for annual Coast Guard compliance inspections and spot checks of their vessels and facilities.
 - d. COTPs shall use this guidance in addition to Coast Guard internal direction to assist industry in implementation of the TWIC Program and in preparation for annual compliance inspections and spot checks of vessels and facilities.
 - e. COTPs are encouraged to bring this circular to the attention of marine transportation interests within their COTP zones. This circular will be distributed by electronic means only. It is available on the World Wide Web at <http://www.uscg.mil/hq/g-m/nvic/index00.htm>.
 - f. The Marine Safety Center, COTPs, and district offices shall use this guidance to review Vessel Security Plan (VSP) and Facility Security Plan (FSP) submissions. Though no vessels are required to submit amendments to their VSP by the TWIC rulemaking, some may choose to do so as allowed by reference (a). The only facilities that are required to submit an amendment to their FSP are those that have a non-transportation portion and voluntarily choose to change their secure area designation.
3. DIRECTIVES AFFECTED. This NVIC provides the guidance needed to implement the new TWIC Program. The information contained herein supplements the guidance contained in previously issued MTSA NVICs and will be incorporated into references (e), (f), and (g) in the future.
4. BACKGROUND.
- a. 46 U.S.C. § 70105, commonly known as MTSA 2002, requires the Secretary of DHS to promulgate regulations to prevent an individual from gaining access to a secure area of a

¹ Note: This population is incorporated into the requirement for all credentialed U.S. Merchant Mariners to possess a TWIC and is not specifically addressed in the TWIC final rule. At this time, we have not extended this requirement to address the issue of non-Federal pilots (those few pilots holding only state commissions or credentials, who do not also hold a federally issued merchant mariner credential). The requirements of 46 U.S.C. 70105(b)(2)(C) [all vessel pilots] will be further addressed in a future notice and comment rulemaking.

² Note: This population is incorporated into the requirement for all vessels subject to 33 CFR part 104 and is not specifically addressed in the TWIC final rule. At this time, we have not extended this requirement to address the issue of all individuals working aboard non-Subchapter H regulated towing vessels that push, pull or haul alongside tank vessels (towing vessels less than or equal to eight meters in registered length and some larger towing vessels that meet the exemptions listed in 33 CFR 104.105). The requirements of 46 U.S.C. 70105(b)(2)(D) [all towing vessels] will be further addressed in a future notice and comment rulemaking.

vessel or facility which has a security plan unless they are authorized to be in the area and hold a “transportation security card” or they are “accompanied by another individual who holds a transportation security card.” The law further states who the law applies to (as listed in Action above), that the individual must be determined not to pose a terrorism security risk, and general requirements for how the determination of terrorism security risk must be carried out. The TWIC regulations were developed from this law.

- b. The TWIC rulemaking, which amended the regulations found in references (a) through (d), requires standardized identification procedures for personnel needing unescorted access to secure areas of facilities and vessels in order to reduce risk and mitigate the effects of a transportation security incident (TSI). This is a joint rulemaking with the Transportation Security Administration (TSA) and the Coast Guard. Reference (a) includes the Coast Guard portions of the TWIC rulemaking while references (b) through (d) include the TSA portions of the rulemaking.
- c. The TWIC Program aims to ensure that only persons who successfully complete a security threat assessment are able to receive a TWIC. The credential will include a reference biometric - fingerprint template - that positively links the credential holder to the identity of the individual to whom the credential was issued. TWIC holders may be asked by a vessel or facility owner or operator or by the Coast Guard to confirm that they are the rightful owner of the credential by providing a fingerprint at any time before being granted unescorted access or during Coast Guard inspection or spot check. In addition, an individual’s credential can be revoked by TSA if disqualifying information is discovered by or presented to TSA or if the credential is lost, stolen, or damaged. Once revoked, the credential should not be used to obtain unescorted access to secure areas. TSA has designed the TWIC process to maintain strict privacy controls so that a holder’s biographic and biometric information is securely protected.

5. DISCUSSION.

- a. Vessels and facilities must be in compliance with the TWIC regulations as discussed in paragraphs 6 b. and c. below, but in no case later than (insert correct date), which is 20 months after the publishing date of the final rule. A detailed implementation plan is contained in Enclosure (5) to this NVIC.
- b. The regulations implementing TWIC require that the TWIC be used initially as a visual identification badge. This means that for normal use at a vessel or facility, the holder’s facial features will be compared to the photo imprinted on the card and the unique identifying surface features of the card will be examined for signs of tampering to identify fraudulent or altered cards. This type of use is more commonly known as a “flash pass”, and is the method that is currently used for checking identification as required by reference (a). During Coast Guard inspections and spot checks, handheld biometric readers will be used to electronically verify that the card is valid (i.e. has not been revoked) and to match the individual to the biometric on the card.
- c. Possession of a TWIC is required to gain unescorted access to secure areas of vessels and facilities. The term “secure area” is defined as “the area over which the owner or operator has implemented security measures for access control in accordance with their security plan.” The terms “secure area” and “restricted area” have different definitions and purposes. Regulations at 33 CFR 101.105 define restricted area as “a location requiring a higher degree of security protection” which is used in a number of regulatory

requirements. A secure area covers a broader space encompassing all restricted areas and includes everything within an access control boundary, as defined in existing security plans. For vessels, the secure area encompasses the entire vessel, with a few exceptions such as passenger access areas and employee access areas. For facilities, the secure area encompasses the entire facility, with the exception of public access areas and those facilities with non-maritime transportation portions who submit an amendment to redefine their secure area. All of these provisions are explained in Enclosure (3).

- d. An individual with a TWIC who is authorized to be in a secure area by the vessel or facility owner or operator is not required to be escorted. An individual who does not have a TWIC must be escorted. Individuals covered under the new hire provision must be continuously accompanied, as opposed to escorted, as is further explained in paragraph 5f.
- e. Escort requirements differ within secure areas depending on whether the area is a restricted area or not. An individual not in possession of a TWIC who is authorized escorted access to a restricted area requires physical, side-by-side accompaniment by a TWIC holder. An individual not in possession of a TWIC who is authorized escorted access by the vessel or facility owner or operator to a secure area that is not also a restricted area requires either physical, side-by-side accompaniment by a TWIC holder or monitoring in a manner sufficient to identify whether the individual is engaged in activities other than those for which escorted access was granted and that allows for quick response. The following communities are likely to need unescorted access to secure areas and will therefore require TWICs (this list is not exhaustive, but is illustrative of those who will likely need a TWIC): vessel crew (in addition to credentialed mariners); longshoremen; drayage truckers and rail crew when handling cargo near a vessel; facility employees if working in a secure area; truckers bringing cargo onto a facility or picking up cargo at a facility. Additional details are provided in Enclosure (2.1) and (3.3).
- f. Newly hired employees (new hires) are able to gain accompanied access to secure areas for up to 30 consecutive days while awaiting issuance of their TWIC. Owners or operators must complete additional steps before new hires may be granted accompanied access. Additional details on this provision are provided in Enclosure (3).
- g. Two non-secure areas have been carved out of the secure area for vessels: the passenger access area and the employee access area. Within these areas, individuals will not be required to possess a TWIC to gain unescorted access. The rest of the vessel remains a secure area for which a TWIC is required for unescorted access. Additional details are provided in Enclosure (3).
- h. The TWIC may be incorporated into existing physical access control systems. If this is done, however, employees must always have their TWIC in their possession and the existing systems should be updated so that they deny access if the TWIC is revoked. Additional details on this provision are provided in Enclosure (3).
- i. Amplification of the knowledge requirements for Company, Vessel, and Facility Security Officers, and for security personnel is provided in Enclosure (3).
- j. If an employee's TWIC is lost, stolen, or damaged, unescorted access to secure areas may be granted for 7 consecutive calendar days while the employee awaits a replacement. Additional steps must be completed by both the employee and the VSO/FSO. These additional details are provided in Enclosure (3).

- k. All credentialed Merchant Mariners may apply for a TWIC at any enrollment center at any time during the 18 month implementation period, but they all must obtain a TWIC by [insert date]. (See 46 CFR 10.xxx and 12.xxx). Until this date, mariners will be allowed to gain unescorted access to secure areas of facilities by providing alternative identification, in lieu of a TWIC. The list of alternative identifications and additional details on this provision are provided in Enclosure (3).
- l. Area Maritime Security (AMS) Committee members are not be required to obtain a TWIC. However, if they have access to SSI, they will be required to undergo name-based security checks, if they do not already possess a TWIC. Additional details are provided in Enclosure (3).
- m. Owners or operators of facilities containing both a marine transportation portion and a non-marine transportation portion, such as areas devoted to manufacturing or refining operations, may voluntarily request a redefinition of their secure area through an amendment to their FSP. COTPs will review and approve these amendments, as appropriate. Additional details regarding the procedures for submitting an amendment are provided in Enclosure (3).
- n. The preamble to the TWIC rule provides additional information regarding the intent of the regulations and is available on the Coast Guard's Homeport website under the Missions/Maritime Security/TWIC heading at <http://homeport.uscg.mil>.

6. IMPLEMENTATION.

- a. TWIC enrollment will begin in selected ports and will expand nationwide over the course of an 18 month period to provide ample opportunity for individuals to apply for and receive their TWIC. Enforcement of the requirement to use TWIC as an access control credential will be based on location and type of operation as explained below. Enrollment and issuance of the TWIC will be carried out by TSA. Enforcement of the TWIC as an access control measure will be carried out by the Coast Guard.
- b. Compliance with this rule for facilities will be phased in by COTP zone in accordance with the following process:
 - (1) A notice will be published in the Federal Register to announce when enrollment begins in each COTP zone.
 - (2) A notice of the compliance date for each COTP zone will be published in the Federal Register. Each notice will be published at least 90 days in advance of the compliance date for its respective COTP zone. In addition, COTPs and the TWIC enrollment contractor will work with port stakeholders to provide notice of the compliance date. This notice may be published in conjunction with the notice which announces the beginning of enrollment.
 - (3) The published compliance date will be the day that all facilities within the specific COTP zone must be in compliance with the requirements in the TWIC rule. It is also the day that Coast Guard enforcement within that COTP zone may begin.
 - (4) A rollout plan, describing implementation across all COTP zones over the 18-month period, is provided in Enclosure (5).
 - (5) The Coast Guard and TSA will also work with AMS Committees and other local forums to communicate compliance dates, enrollment center locations, and other vital information to maximize the availability of this information to stakeholders.

- c. Compliance with this rule for vessels is no later than [INSERT DATE – 20 mo after publishing date of rule]. By [INSERT DATE – same date], all U.S. credentialed Merchant Mariners will be required to present a TWIC for unescorted access to vessels and facilities. Until then, if the vessel or COTP zone where they are operating has started TWIC compliance and enforcement, mariners may present an alternate identification as necessary to gain unescorted access to secure areas of facilities. Alternative mariner identifications are listed along with additional details in Enclosure (3).
 - d. A vessel or facility not implementing a TWIC Program after the published compliance dates is subject to civil penalty action and may be subject to additional control and compliance measures, including suspension of facility or vessel operations [see Enclosure (4)].
 - e. Enclosure (1) is a TSA produced flowchart of the TWIC enrollment and issuance process.
 - f. Enclosure (2) is a TSA publication that provides more detail and guidance for the enrollment and issuance process.
 - g. Enclosure (3) provides guidance on facility and vessel implementation.
 - h. Enclosure (4) provides guidance on enforcement of the TWIC requirements.
 - i. Enclosure (5) is the implementation schedule for enrollment nationwide.
7. INFORMATION SECURITY. TWIC credentials and associated databases contain sensitive personal information that, if released to the general public or improperly accessed or used by personnel executing their official duties, could compromise the privacy of an individual. This information shall be protected under the requirements of the Privacy Act, 5 U.S.C. 552a.
8. DISCLAIMER. While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State agencies in understanding the TWIC statutory and regulatory requirements, this guidance is not a substitute for the applicable legal requirements, nor is it in itself a rule. It is not intended to nor does it impose legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.
9. CHANGES. This NVIC will be posted on the web at www.uscg.mil/hq/g-m/nvic/index00.htm and Homeport at <http://homeport.uscg.mil>. Changes to this circular will be issued as necessary. Time-sensitive amendments will be issued as “urgent change” messages to COTPs and posted on the website for the benefit of industry, pending their inclusion to the next change to this circular. Suggestions for improvement of this circular should be submitted in writing to Commandant (CG-3PC).

B. M. SALERNO
Rear Admiral, U.S. Coast Guard
Director of Inspections and Compliance

- Encl: (1) TWIC Enrollment and Issuance Process Flowchart
(2) Enrollment and Issuance Process Description
(3) TWIC Program Implementation for Vessels and Facilities

- (4) Enforcement Guidance
- (5) Implementation Schedule from TSA Contractor

DRAFT

Implementation Guidance for the Transportation Worker Identification Credential; Enrollment and Issuance

Table of Contents

Enclosure (1) — TWIC Enrollment and Issuance Process Flowchart

Enclosure (2) — Enrollment and Issuance Process Description

- 2.1 Who must get a TWIC?
- 2.2 Who can apply for a TWIC?
- 2.3 What happens to my TWIC when my lawful nonimmigrant status expires?
- 2.4 What can disqualify me from getting a TWIC?
- 2.5 What if I do not meet the qualification standards?
- 2.6 TWIC Enrollment
 - Owner Or Operator Notification Requirement
 - Location and Timing
 - Enrollment Process
 - (1) Pre-Enrollment
 - (2) Enrollment
 - (3) Fee Collection
 - (4) Security Threat Assessment and Notification
 - (5) TWIC Issuance
- 2.7 Waivers and Appeals
- 2.8 Privacy and Information Security
- 2.9 TWIC Call Center
- 2.10 TWIC Renewal
- 2.11 Lost, Stolen or Damaged TWICs

Enclosure (3) – TWIC Program Implementation for Vessels and Facilities

- 3.1 TWIC Applicability
 - a. Vessels
 - b. Facilities
- 3.2 TWIC Implementation Schedule
 - a. Enrollment
 - b. Compliance
- 3.3 Vessel and Facility Guidance
 - a. Access Control – Using TWIC as a Visual Identity Badge
 - b. Secure Areas
 - c. Escorting
 - d. Employee Notification Requirement
 - e. Incorporation of the TWIC Procedures into Security Plans
 - f. Incorporation of the TWIC into Existing Physical Access Control Systems
 - g. Knowledge Requirements for Personnel
 - h. Special Provisions for Access Control
 - i. TWIC Procedures Remain the Same Regardless of MARSEC Level
 - j. Area Maritime Security Committee Members

- k. Waivers, Exemptions, and Equivalencies of TWIC Requirements
- 3.4 Facility-specific Guidance
 - a. Amendment of FSPs to Designate Certain Portions of the Facility as Secure Areas for TWIC
 - b. Amendment Procedures for Redefining Secure Areas
- 3.5 Vessel-specific Guidance
 - a. Passenger and Employee Access Areas
 - b. Vessels not Eligible for Redefinition of Secure Areas

Enclosure (4) – Enforcement Guidance

- 4.1 Enforcement Strategy
- 4.2 Enforcement Implementation
- 4.3 Invalid/Fraudulent Cards
 - a. Owner or Operator Actions
 - b. Possible Coast Guard Actions

Enclosure (5) – Implementation Schedule



Enclosure (1) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 07-XX

This diagram depicts the process of applying for and obtaining a TWIC. More information is available by viewing the references to the Navigation and Inspection Circular (NVIC) pages and Code of Federal Regulations (CFR) sections included in each box. Other information is available at <http://www.tsa.gov/twic> and <http://homeport.uscg.mil>.

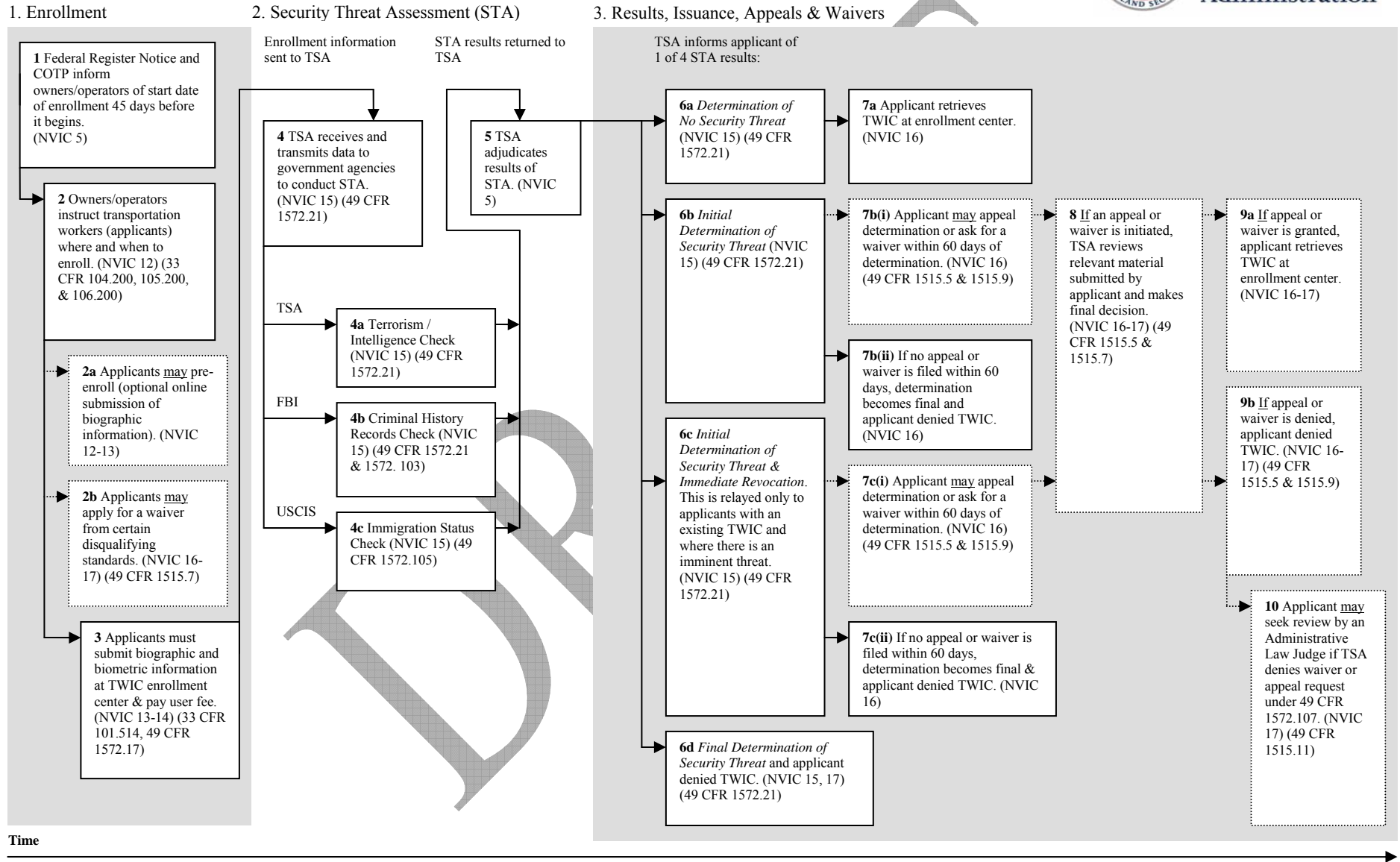


Table of Contents

Enclosure (2) – Enrollment and Issuance Process Description

	Page
2.1 Who must get a TWIC?	12
2.2 Who can apply for a TWIC?	12
2.3 What happens to my TWIC when my lawful nonimmigrant status expires?	13
2.4 What can disqualify me from getting a TWIC?.....	13
2.5 What if I do not meet the qualification standards?	13
2.6 TWIC Enrollment	14
Employee Notification Requirement	14
Location and Timing	14
Enrollment Process	14
(1) Pre-Enrollment	15
(2) Enrollment.....	15
(3) Fee Collection	16
(4) Security Threat Assessment and Notification	17
(5) TWIC Issuance.....	17
2.7 Waivers and Appeals	18
Waivers	18
Appeals	19
2.8 Privacy and Information Security	19
2.9 TWIC Call Center.....	19
2.10 TWIC Renewal	19
2.11 Lost, Stolen, or Damaged TWICs.....	20

Enclosure (2) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 07-XX

U.S. Department of Homeland Security
Arlington, VA 22202



**Transportation
Security
Administration**

Enrollment and Issuance Process Description

2.1 Who must get a TWIC?

- Merchant mariners and individuals who will need unescorted access to secure areas of a vessel or facility will need to obtain a TWIC. The vessel or facility owners or operators determine who will need unescorted access to the secure area(s) of their vessel or facility. Owners or operators can require escorted access of a TWIC holder if they choose to do so. Possession of a TWIC does not guarantee unescorted access to secure areas; permission must also be granted by the vessel or facility. The following communities are likely to need unescorted access to secure areas and will therefore require TWICs (this list is not exhaustive, but is illustrative of those who will likely need a TWIC):
 - Vessel crew (in addition to credentialed mariners).
 - Longshoremen.
 - Drayage truckers and rail crew when handling cargo near a vessel.
 - Facility employees if working in a secure area.
 - Truckers bringing cargo onto a facility or picking up cargo at a facility.

2.2 Who can apply for a TWIC?

The following individuals are eligible to apply for a TWIC 49 CFR 1572.105:

- a. A national of the United States.
- b. A lawful permanent resident of the United States.
- c. A refugee admitted under 8 U.S.C. 1157.
- d. An alien granted asylum under 8 U.S.C. 1158.
- e. An alien in valid M-1 nonimmigrant status who is enrolled in the United States Merchant Marine Academy or a comparable State maritime academy. Such individuals may serve as unlicensed mariners on a documented vessel, regardless of their nationality, under 46 U.S.C. 8103.
- f. A nonimmigrant alien admitted under the Compact of Free Association between the United States and the Federated States of Micronesia, the United States and the Republic of the Marshall Islands, or the United States and Palau.
- g. A commercial driver licensed in Canada or Mexico who is admitted to the United States under 8 CFR 214.2(b)(4)(i)(E) to conduct business in the United States.
- h. An alien in lawful nonimmigrant status who has unrestricted authorization to work in the United States, except—
 - (1) An alien in valid S-5 (informant of criminal organization information) lawful nonimmigrant status;

- (2) An alien in valid S-6 (informant of terrorism information) lawful nonimmigrant status;
 - (3) An alien in valid K-1 (Fiancé(e)) lawful nonimmigrant status; or
 - (4) An alien in valid K-2 (Minor child of Fiancé(e)) lawful nonimmigrant status.
- i. An alien in the following lawful nonimmigrant status who has restricted authorization to work in the United States—
- (1) H-1B Special Occupations;
 - (2) H-1B1 Free Trade Agreement;
 - (3) E-1 Treaty Trader;
 - (4) E-3 Australian in Specialty Occupation;
 - (5) L-1 Intracompany Executive Transfer;
 - (6) O-1 Extraordinary Ability; or
 - (7) TN North American Free Trade Agreement.

2.3 What happens to my TWIC when my lawful nonimmigrant status expires?
The applicant must report the disqualifying condition to TSA and surrender the TWIC. In addition, the TWIC becomes invalid.

If the applicant is in one of the permissible visa categories listed in 2.2(i), and the employment for which the visa was granted ends:

- the employer retrieves the TWIC from the applicant and provides it to TSA.
- the applicant surrenders the TWIC to the employer.
- If an employer terminates an applicant working under a nonimmigrant status listed in paragraph 2.2(i), or the applicant otherwise ceases working for the employer, the employer must notify TSA within 5 business days and provide the TWIC to TSA if possible.

2.4 What can disqualify me from getting a TWIC?

- Criminal – an individual has been convicted or incarcerated for certain crimes within prescribed time periods.
- Immigration – an individual does not meet the immigration status requirements listed in 49 CFR 1572.105.
- Security threat – an individual is identified as having a connection to terrorist activity.
- Mental incapacity – an individual is or has been determined to lack mental capacity as defined in 49 CFR 1572.109.

2.5 What if I do not meet the qualification standards?

- All applicants have the opportunity to appeal an Initial Determination TSA makes that an applicant does not meet the standards. TSA provides applicants the reason for the Initial Determination and instructions on how to apply for an appeal. If an applicant knows that he or she does not meet the standards concerning criminal activity or mental capacity, or is in Temporary Protected Status at the time enrollment, the applicant should check the box on the enrollment form “applying for a waiver.” If the applicant becomes aware that he or she does not meet the standards concerning criminal activity or mental capacity when TSA issues an Initial Determination, the applicant may apply for a waiver at that time.

2.6 TWIC Enrollment

Employee Notification Requirement

- Facility and vessel owners or operators, under 33 CFR 104.200, 105.200, and 106.200 in the TWIC rule, are required to inform facility and vessel employees of their responsibility to possess a TWIC and what parts of the facility and vessel are secure areas, passenger access areas, employee access areas, and public access areas. The intent of this requirement is for owners or operators to determine which of their employees will need a TWIC and inform those employees in enough time for them to comply with the requirements. Owners and operators are also encouraged, but not required, to provide this same information to personnel who are not facility or vessel employees, e.g. contractors.
- Notification should assist the employee in determining the following:
 - his/her responsibility to possess a TWIC;
 - if he/she will need unescorted access to a secure area;
 - what parts of the facility or vessel are public, employee, or passenger access areas;
 - when compliance will begin in his/her COTP zone; and
 - locations of enrollment centers where he/she can apply for his/her TWIC.
- Some acceptable forms of notification include the following examples:
 - Signs posted in common areas
 - Company newsletters
 - Announcements by company officials
 - Company website
 - Inserts in wage and salary statements or other payroll documents

Location and Timing

- Approximately 130 ports have been identified for enrollment sites. TSA will use a combination of fixed and mobile enrollment stations to make the enrollment process as efficient as possible for applicants and owners or operators. The TSA enrollment contractor is responsible for identifying the specific enrollment sites. The enrollment locations and directions to these sites will be available on the TWIC website at www.tsa.gov/twic.
- TSA and Coast Guard will work closely with the maritime industry to ensure that owners or operators and applicants are given as much notice as is possible of the commencement of enrollment at their location. See Enclosure (3) and 49 CFR 1572.19 of the final rule for more details.

Enrollment Process

- The enrollment process consists of 5 components: pre-enrollment (optional), enrollment, fee collection, security threat assessment and notification of the results, and issuance of the TWIC to the applicant. The time from enrollment to credential availability is expected to take less than 30 days, not including potential appeal or waiver processing. If the security threat assessment does not reveal any questionable or negative information about an individual, the process is expected to take less than 10 days.

(1) Pre-Enrollment

- Applicants are encouraged, but not required, to “pre-enroll” online at www.tsa.gov/twic. The pre-enrollment process allows applicants to provide much of the biographic information required for enrollment; to select an enrollment center where they wish to complete enrollment; and to make an appointment to complete enrollment at the enrollment center of their choosing.
- The benefits of pre-enrollment include:
 - May reduce the time needed to complete the entire enrollment process at an enrollment center.
 - Allows applicants to provide much of the biographic information required for enrollment from home or another convenient location.
 - Provides the list of documents to bring to the enrollment center for identity verification and other purposes.
 - Provides the privacy statement that will be signed at enrollment.
 - Provides the enrollment site locations and hours of operation.
 - Provides applicants the opportunity to make an appointment at an enrollment center. Although applicants may schedule an appointment to complete enrollment at an enrollment center, appointments are not required.
- Applicants may pre-enroll from any computer with Internet access. The web site for pre-enrollment and additional information relating to the TWIC program will be available from www.tsa.gov/twic. This web site also will list the documents the applicant must bring to the enrollment center to verify identity and for other purposes so that all applicants can be properly prepared.

(2) Enrollment

- During enrollment, applicants will be required to visit the enrollment center to provide biographic information and a complete set of fingerprints, sit for a digital photograph, and pay the enrollment fee. Regardless of whether the applicant pre-enrolls, the applicant must bring identity verification documents and in the case of aliens, immigration documents to the enrollment center so that they can be scanned into the electronic enrollment record. The list of required documents an applicant must present will be posted on the TWIC website at www.tsa.gov/twic.
- Applicants must sign the enrollment documents at the enrollment center.
- All U.S. credentialed Merchant Mariners must provide proofs of citizenship and/or alien status required by the Coast Guard at 46 CFR Chapter I, Subchapter B, to TSA at the time of TWIC enrollment. TSA will scan these documents into the enrollment record and provide them to the Coast Guard for use in evaluating applicants for original or renewal merchant mariner’s licenses, merchant mariner’s documents, certificates of registry, Standards of Training, Certification and Watchkeeping (STCW) endorsements, and if the Coast Guard begins to issue them, merchant mariner credentials. Requiring this information to be submitted at TWIC enrollment allows the Coast Guard to remove the requirement that all mariners travel to one of the 17 Coast Guard Regional Exam Centers to submit this information.
- All applicants will receive a disclosure form when they enroll, by which they agree to provide personal information for the security threat assessment and credential. If an applicant fails to sign the disclosure form or does not have the required documents to

authenticate identity, enrollment will not proceed. For applicants who pre-enroll, the privacy notice is provided with the application on-line, but the applicant must acknowledge receipt of the notice in writing at the enrollment center.

- Applicants will provide a complete set of fingerprints and sit for a digital photograph. Fingerprints will be used for the security threat assessment and to create the template for the biometric information stored on the credential and the photograph will be placed on the TWIC card for identification purposes. Fingerprinting will consist of 10 fingers unless the applicant has lost or seriously injured his or her fingers. Alternative procedures will be used for applicants who cannot provide any fingerprints. The fingerprints and photograph will be electronically captured at the enrollment center and made part of the applicant’s TWIC enrollment record.
- Applicants who know they do not meet the qualification standards due to criminal activity or mental incapacity, or are aliens in Temporary Protective Status and wish to use the waiver process may initiate it during enrollment.
- Information on the TSA website www.tsa.gov/twic contains guidance on the process.

(3) Fee Collection

- Applicants will pay a fee in accordance with the following table (*note: approximate ranges are listed -- exact fee will not be determined until deployment contract is awarded*):

Category	Fee
Individuals requiring a security threat assessment	\$139-\$159
Individuals not requiring a security threat assessment (i.e. Hazardous Materials endorsement issued after 5/31/2005, FAST card, or MMD issued after 2/3/2003 or Merchant Mariner license issued after 1/13/2006)	\$107-\$127
Card replacement fee (lost, stolen, or damaged).	\$36 * Proposed to be increased to \$60

- The fee, which covers the cost of enrollment, security threat assessment, and credential production and delivery, will be collected from the applicant at enrollment. Payment can be made by cashier’s check, money order, or credit card. The TWIC enrollment fee is non-refundable, even if the threat assessment results in denying the applicant a TWIC.
- Applicants who have completed a comparable threat assessment (hazardous materials endorsement, FAST card, merchant mariner’s document (MMD), certificate of registry, or merchant mariner license) and wish to pay a reduced TWIC fee because they do not need another threat assessment, must present their hazardous materials endorsement, FAST card, MMD, certificate of registry, or merchant mariner license at enrollment. The TWIC expiration date for FAST, MMD, certificate of registry, and merchant mariner license holders will be five years from the date of those

credentials were issued. The TWIC expiration date for Hazardous Materials Endorsement holders will be five years from the date of the HME issuance.

(4) Security Threat Assessment and Notification

- TSA will conduct a security threat assessment on all applicants consisting of the following components in order to determine whether or not the individual poses a security threat:
 - Fingerprint-based criminal history records check (CHRC).
 - Intelligence-related check to identify potential ties to terrorism.
 - Immigration status.
- The applicant will be notified of the results of the threat assessment as follows:
 - 1) Determination of No Security Threat (TWIC is ready for pick-up): via email or telephone, whichever method the applicant selects on the application.
 - 2) Initial Determination of Threat Assessment: via mail.
 - 3) Initial Determination of Threat Assessment and Immediate Revocation: via mail.
 - 4) Final Determination of Threat Assessment: via mail.
- In the case of 2) and 3) above, the notification will include a written statement that the applicant may pose or poses a security threat warranting denial of the TWIC, the basis for the determination, information on how to appeal the determination, seek a waiver or request materials, and a statement that if the applicant does not reply to TSA within the time period (60 days) the Initial Determination of Threat Assessment will become a Final Determination of Threat Assessment. See Waivers and Appeals section below for more information.
- The Final Determination of Threat Assessment is served to the individual and, in the case of a mariner, also to the Coast Guard.
- If the applicant decides to appeal the Initial Determination of Threat Assessment or the Initial Determination of Threat Assessment and Immediate Revocation, then the procedures in 49 CFR part 1515 apply.
- If TSA determines that an applicant poses an imminent threat, TSA may notify the applicant's employer. Generally, TSA will not provide the reasons for a disqualification to an employer. However, if TSA has reliable information concerning an imminent threat posed by an applicant and providing limited threat information to an employer, facility, vessel owner, or COTP would minimize the risk, then TSA would provide such information.

(5) TWIC Issuance

- As stated above, an applicant who has received a 'Determination of No Security Threat' will be notified, by email or phone, as indicated on their application, when their credential is available at the enrollment center. The applicant must return to the same enrollment center where they enrolled to activate and pick up the TWIC.
- At the enrollment center, the photograph and name on the card are compared to the applicant and the identity documents presented by the applicant to authenticate their identity. The applicant places a designated finger on a reader to perform a biometric verification with the biometric template stored on the credential and in the TSA system.

- Upon successful biometric match, the applicant selects a personal identification number (PIN) that is stored on the credential. The PIN can subsequently be used as an additional security device to authenticate identity and authorize use of the credential. The PIN can also be used as the primary verification tool if the biometric is inoperative.
- Once the enrollment and issuance process is completed, the credential is activated and is ready to be presented at a facility or vessel for use as an access control tool.
- The TWIC security threat assessment and credential are valid for five years, except where of the TWIC is based on a previous comparable security threat assessment. TSA will conduct perpetual vetting on all TWIC holders throughout the 5 year life of the credential. If TSA discovers information that disqualifies the applicant, TSA will revoke the credential. Additionally, applicants are required to notify TSA if they have been convicted of a disqualifying offense or no longer meet the immigration standard.

2.7 Waivers and Appeals

- All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes or mental incapacity, or are aliens in Temporary Protected Status. Applicants who are denied a TWIC will be provided with information on why they were denied a TWIC and instructions on how to apply for an appeal or waiver.
- *Waivers*
 - TSA has designed a waiver process that is informal, designed for applicants who are not represented by counsel and not conversant with legal terms and processes. TSA accepts hand-written applications, so the applicant does not need to have a computer.
 - Applicants are encouraged to initiate the waiver process at the time of enrollment if they know they will not meet the standards and are eligible for a waiver. The TSA website (www.tsa.gov/twic) contains guidance on the process. The applicant has 60 days from the time they receive a Final Determination of Threat Assessment to provide the required information to TSA for consideration.
 - When completing the waiver request, the applicant should describe why he or she no longer poses a security threat. Information that assists TSA with this determination includes:
 - the circumstances surrounding the conviction.
 - the applicant's work and personal history since the conviction.
 - the length of time the applicant has been out of prison if sentenced to incarceration.
 - references from employers, probation officers, parole officers, clergy and others who know the applicant and can attest to his or her responsibility and good character.
 - Applicants denied due to mental incapacity may also apply for a waiver. Court records or official medical release documents that state the applicant no longer lacks mental capacity will be considered in the waiver, although are not always necessary to obtain a waiver.

- If TSA denies an applicant's waiver request, the applicant may seek review of the decision by an Administrative Law Judge (ALJ).

Appeals

- The appeal process is available to all applicants if they believe TSA has not applied the standards appropriately or has based its security threat assessment determination on incorrect court records or mistaken identity. Applicants who file an appeal may supply the correct records to TSA.
- Following TSA's Initial Determination, an applicant initiates an appeal by requesting documents from TSA, responding to TSA, or providing TSA with corrected records or other proof that the Initial Determination was based on erroneous court records or mistaken identity.
- Applicants who are disqualified due to the intelligence-related check and appeal unsuccessfully may seek review from an Administrative Law Judge.

2.8 Privacy and Information Security

- Privacy and information security are critical to the TWIC program. Information collected at the enrollment center or during the pre-enrollment process, including the signed disclosure form and identity documents, is scanned into the TWIC system for storage. Information is encrypted or stored using methods that protect the information from unauthorized retrieval or use.
- The fingerprint images collected from each applicant will be submitted to the FBI for the criminal history records check. The images of two of the fingerprints will be converted to fingerprint minutiae templates, not the actual fingerprint, and used on the credential as the reference biometric to verify identity.
- The entire enrollment record (including all fingerprints collected) will be encrypted, transmitted to the central database, and segmented to prevent unauthorized use. The TSA system acknowledges receipt of the enrollment record, at which time all enrollment data is automatically deleted from the enrollment workstation.
- Additional information on this topic is also available in the TWIC Privacy Impact Assessment (PIA) which is available on TSA's website.

2.9 TWIC Call Center

- A toll-free TWIC Call Center (phone number available once TWIC deployment contract is awarded) support provides around-the-clock service for merchant mariners, transportation workers, facility and vessel owners and operators, and others who require assistance related to the TWIC program. Additional information on the Call Center will be available at www.tsa.gov/twic.
- Assistance includes help for enrollment; lost, stolen, or damaged cards; PIN resets (note: an applicant will have 10 tries to get their PIN correct if they forget it); etc. Help is also available for scheduling enrollment appointments, locating the closest enrollment facility to an applicant, and guiding applicants through the web-based pre-enrollment process.

2.10 TWIC Renewal

- Generally, TWICs remain valid for five years, unless renewed before the five-year term ends. Upon renewal, an applicant receives a new credential and the old credential is invalidated in the TSA System. TSA does not plan to notify TWIC holders when their credential is about to expire because the expiration date is displayed on the face of the credential.
- If the applicant paid a reduced fee for a TWIC based on an earlier comparable threat assessment and credential (FAST, HME, MMD), the TWIC will expire five years from the date of the comparable threat assessment and credential.
- To renew a TWIC, the holder must appear at any enrollment center. Mariners are urged to start the renewal process approximately 180 days before the expiration date of the credential to accommodate Coast Guard processing of mariner qualifications. All other applicants should apply at least 30 days prior to expiration in order to facilitate timely processing of the TWIC renewal.
- When renewing the TWIC, applicants must again provide biographic and biometric information and identity verification documents, and pay the associated fees. Note that the TWIC web site will maintain a list of documents that may be used to verify identity, which may change over time.
- TSA issues a new credential once the enrollment process and threat assessment is complete. The expired credential will be deactivated. The new credential will expire five years from the date of issuance. Although renewal occurs every five years, TSA conducts recurring name-based security threat assessments on applicants throughout the five year period.

2.11 Lost, Stolen, or Damaged TWICs

- Applicants who determine that their TWIC is lost, stolen or damaged should contact the TWIC Call Center immediately (placeholder for phone number).
- After the applicant reports the card as lost, stolen, or damaged, the Call Center will contact the card production facility to trigger production of a replacement TWIC. The replacement credential will be sent to the enrollment center designated by the applicant.
- TSA will add the lost, stolen, or damaged credential to the list of revoked cards to decrease the chance that the credential could be used by an unauthorized person to gain unescorted access. Once the replacement TWIC arrives at the enrollment center, the applicant will can pick it up and pay the card replacement fee of \$36. (We are proposing to increase this fee to \$60.)
- The replacement card will have the same expiration date as the original.

Table of Contents

Enclosure (3) – TWIC Program Implementation for Vessels and Facilities		Page
3.1	TWIC Applicability	22
a.	Vessels	22
b.	Facilities	22
3.2	TWIC Implementation Schedule	22
a.	Enrollment	22
b.	Compliance	23
3.3	Vessel and Facility Guidance	23
a.	Access Control – Using TWIC as a Visual Identification Badge	23
b.	Secure Areas	25
c.	Escorting	27
d.	Employee Notification Requirement	29
e.	Incorporation of the TWIC Procedures into Security Plans	30
f.	Incorporation of the TWIC into Existing Physical Access Control Systems	30
g.	Knowledge Requirements for Personnel	31
h.	Special Provisions for Access Control	32
i.	TWIC Procedures Remain the Same Regardless of MARSEC Level	36
j.	Area Maritime Security (AMS) Committee Members	36
k.	Waivers, Exemptions, and Equivalencies of TWIC Requirements	37
3.4	Facility-specific Guidance	38
a.	Amendment of FSPs to Designate Certain Portions of the Facility as Secure Areas for TWIC	38
b.	Amendment Procedures for Redefining Secure Areas	38
3.5	Vessel-specific Guidance	38
a)	Passenger and Employee Access Areas	38
b)	Vessels not Eligible for Redefinition of Secure Areas	39

Enclosure (3) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 07-xx

TWIC Program Implementation for Vessels and Facilities

3.1 TWIC Applicability

a. Vessels

- (1) The TWIC access control requirements apply to U.S.-flagged vessels subject to 33 CFR Part 104 only.
- (2) U.S. vessels operating under the waivers provided for under 46 U.S.C. 8103(b)(3)(A) or (B) do not have secure areas and therefore are not required to observe TWIC access control requirements. This waiver allows offshore supply vessels and mobile offshore drilling units (or similar vessels) to employ foreigners as crew when operating from a foreign port or beyond the Outer Continental Shelf. See United States Code for details on this waiver. However, when these vessels are not operating under these waivers (i.e. within the U.S. Outer Continental Shelf and shoreward), they do have secure areas and are required to comply with TWIC requirements. All other U.S.-flagged vessels will be required to comply with the TWIC requirements regardless of location.
- (3) TWIC requirements will not apply to foreign-flagged vessels subject to 33 CFR Part 104.
- (4) The TWIC requirements do not apply to mariners on U.S. facilities working immediately adjacent to the vessels they are employed aboard while in the conduct of vessel activities. This allows both mariners limited access to the area immediately adjacent to their vessels to conduct operations in support of the vessel (i.e. to attach shore ties, perform maintenance, remove trash, etc.). This provision may be used by both foreign mariners and U.S. mariners, onboard vessels not subject to 33 CFR part 104 who would not otherwise be required to possess a TWIC.

b. Facilities

The TWIC access control requirements apply to all facilities subject to 33 CFR Part 105 and 106.

3.2 TWIC Implementation Schedule

a. Enrollment

TWIC implementation will begin with the establishment of TWIC enrollment centers. These are contractor-operated locations that enroll members and issue TWICs in accordance with the procedures described in Enclosure (2). Enrollment will begin with the establishment of centers in several ports and then will expand to provide enrollment centers in approximately 130 ports nationwide during the TWIC phase-in period. Enrollment phase-in will be complete when all workers requiring a TWIC have had ample opportunity to enroll and when use of the TWIC becomes mandatory in all locations nationally, at the end of 18 months. Enrollment center locations and staff will

then be reduced as appropriate to manage the enrollment of new individuals entering the maritime-related workforce, lost, stolen, or damaged TWIC replacements, and TWIC renewals. Enrollment centers will remain in locations convenient to the centers of regulated port facility and vessel activity after the 18 month phase-in period. A current schedule of enrollment center phase-in is posted at [include website when contract is awarded]. The schedule of the roll out of enrollment centers nationally may change during the roll out process, so individuals need to check this website in order to get up-to-date information.

b. Compliance

(1) Facilities

Compliance with TWIC will be phased in on a COTP zone basis. Each zone’s compliance date will be based upon when COTP zone enrollment begins. Compliance dates will be announced in the Federal Register at least 90 days before coming into effect. See Enclosure (5) for a detailed enrollment schedule.

(2) Vessels

Because operations of individual vessels may not be limited to single COTP zones, vessel owners and operators will not be required to implement TWIC on a phased-in basis. Instead, vessel owners and operators are required to comply with TWIC requirements no later than [insert date], 20 months after the publishing date of the final rule. However, owners and operators of vessels that operate exclusively within a single COTP zone may have vessel employees enroll for and use TWICs as an access control measure as their COTP zone comes into compliance. This will facilitate unescorted access for these individuals through facilities that have implemented TWIC access control requirements, though mariners may gain unescorted access by showing an alternative identification. See paragraph 3.3 h. (3) (b) for additional information on merchant mariner unescorted access through regulated facilities during the TWIC phase-in period.

Type of operation	Compliance Date
Vessels (33 CFR 104)	20 mo after pub date [insert date]
Facilities (33 CFR 105)	by COTP zone – date published in Federal Register
OCS Facilities (33 CFR 106)	by COTP zone – date published in Federal Register
Merchant Mariners	20 mo after pub date [insert date]

3.3 Vessel and Facility Guidance

a. Access Control – Using TWIC as a Visual Identification Badge

(1) The TWIC will be employed as a visual identification badge in order for an individual to be granted unescorted access to a secure area. The vessel or facility must conduct a positive verification of the TWIC before allowing unescorted access to a secure area(s). Typically, such positive verification will take place at an access control point, beyond which only properly credentialed individuals are permitted to enter without escort. The TWIC does not need to be worn on clothing, but must be available for inspection if requested by security personnel or Coast Guard inspectors.

- (2) The TWIC incorporates a number of readily identifiable, tamper indicating security features that make alteration or forgery of the credential difficult. Security personnel, tasked with inspecting the TWIC, must be familiar with these security features, knowledgeable in credential verification, and the procedures to follow should a TWIC be presented which does not appear to have all of the established features [see Enclosure (4)]. Alternative verification methodologies (e.g. camera to see identification from trucking lane) may continue to be made electronically, from a remote location (e.g. security checkpoint), in accordance with provisions specifically described and approved in the current vessel and/or facility security plan or provided for in an approved revision. However, in order to be employed, these methodologies must allow for the security features of the TWIC to be readily identified. TWIC verification processes must include the following provisions for credential verification:
- (1) A match of the photo on the TWIC to the individual presenting the TWIC;
 - (2) Verification that the TWIC has not expired; and
 - (3) A visual check of the various security features present on the credential to ensure that the TWIC has not been forged or tampered with.

Placeholder for new TWIC images...

1	Front	Description of TWIC security features here...
2	Front	
3	Front	
4	Back	
5	Front	

6	Front	
7	Front	
8	Front	

b. Secure Areas

- (1) The foundation of the TWIC Program is the definition of the secure area. The terms “secure area” and “restricted area” do not mean the same thing. A secure area is defined as “the area over which an owner/operator has implemented security measures for access control” to reduce the probability of a TSI. The secure area is the entire area within the outer-most access control perimeter of a facility, with the exception of public access areas, and encompasses all restricted areas. The secure area is bound by the fence line or other barrier, waterfront, and gates, which also provide access to the secure area. It also encompasses the entirety of a vessel or OCS facility because access control is conducted at the gangway or embarkation point, with the exception of passenger or employee access areas for vessels (see discussion in section 3.5). The secure area is the area encompassed by the approved security plan, except in the case of facilities with a non-transportation component if they submit an amendment to their FSP to redefine the secure area to include only the transportation section of the facility (see discussion in section 3.4).
- (2) Restricted areas fall within this perimeter and are already defined in reference (a) as “the infrastructure 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.” (33 CFR 101.105) Restricted areas of a vessel or facility present a heightened opportunity for a TSI. Additionally, reference (a) spells out certain areas within vessels and facilities that must be included as restricted areas (see 33 CFR 104.270, 105.260, and 106. 265).
- (3) Figures below show one representation each of secure areas as the following types of facilities and vessels:
 - Figure 1 - Marine terminal, wholly transportation related
 - Figure 2 - Marine terminal, some non-maritime transportation portions after amendment for redefinition of secure area to FSP approved
 - Figure 3 - Cargo vessel
 - Figure 4 - Passenger vessel

These representations are for illustrative purposes only and do not supersede the regulations. Each facility and vessel is unique and these diagrams serve merely to provide a visual representation of the secure and restricted areas and are not meant to cover all possible arrangements.

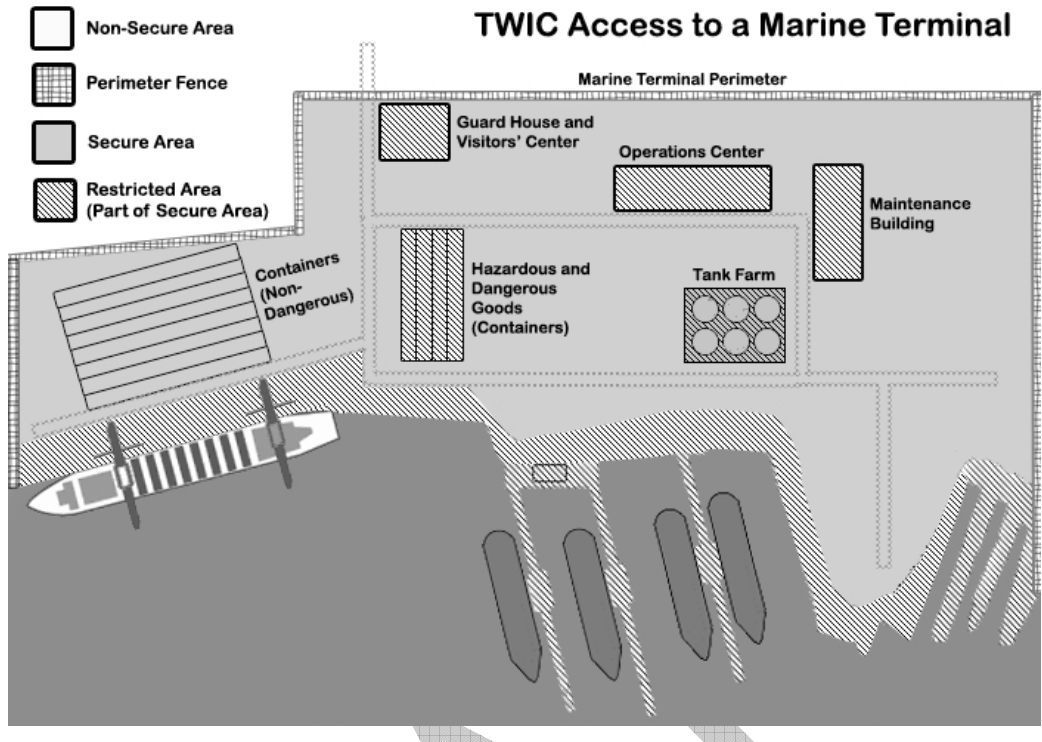


Figure 1 - Marine terminal, wholly transportation related

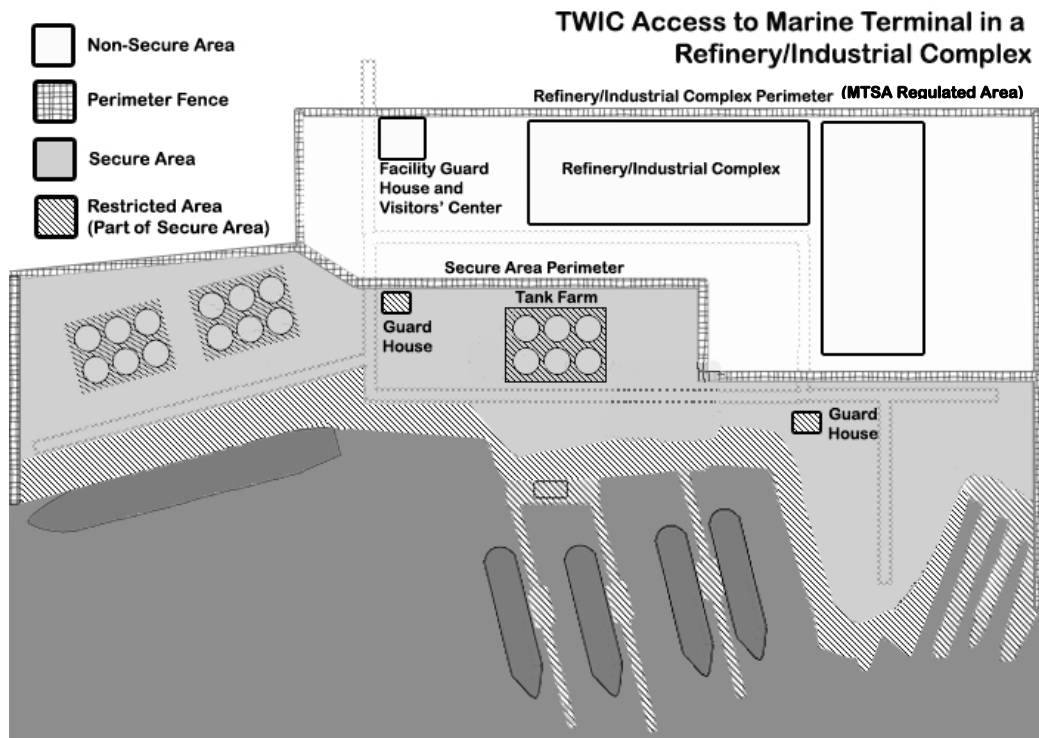


Figure 2 - Marine terminal, some non-maritime transportation portions

TWIC Access on a Cargo Vessel

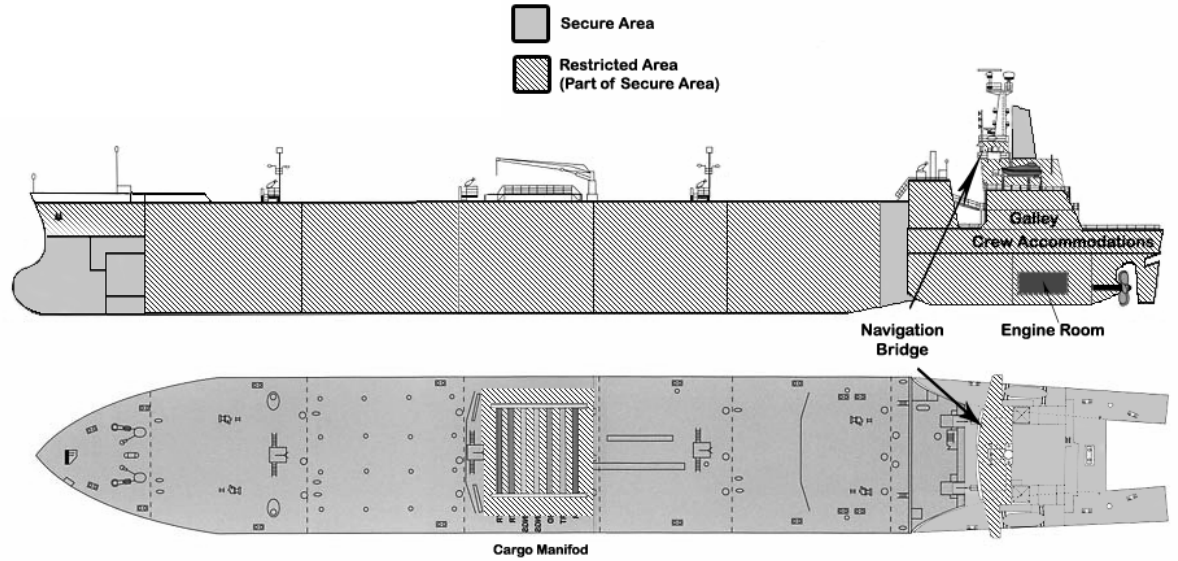


Figure 3 – Cargo vessel

TWIC Access on a Passenger Vessel

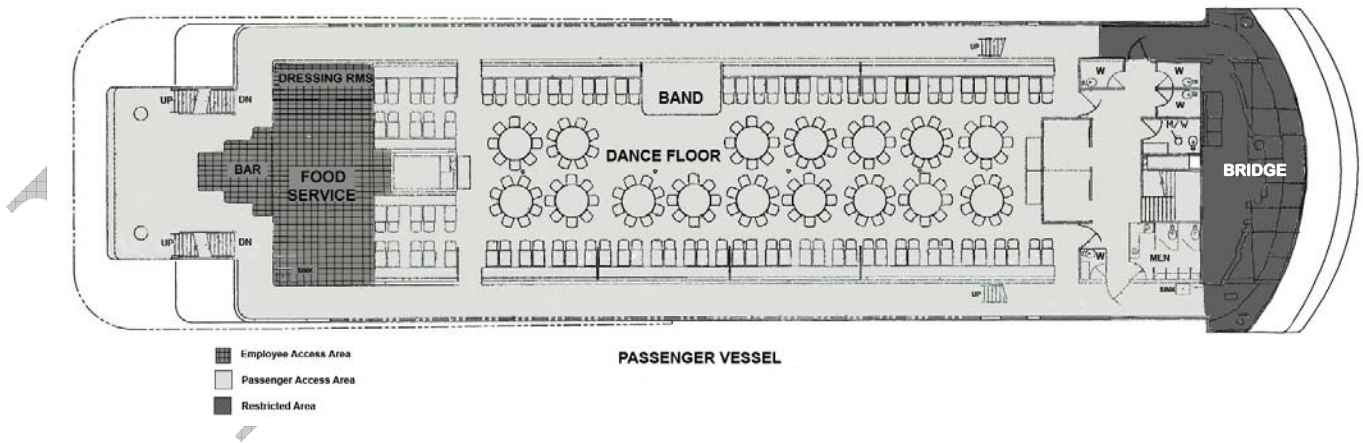


Figure 4 - Passenger vessel

c. Escorting

- (1) The purpose of the TWIC Program is to ensure that only individuals who possess a TWIC are granted unescorted access to secure areas. This means that those who do not possess a TWIC but still have a need to enter the secure area must be escorted. As defined in the regulations, 33 CFR 101.105, “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. There are two specific escort categories (see table below): (1) escort within secure areas that are not also restricted areas and (2) escort within portions of the secure areas that are restricted areas. There are also separate requirements for new hires, which supersede the escorting requirements when used.
- (2) Escorting in secure but nonrestricted areas: escorting must be accomplished in one of two ways: monitoring, as described in 33 CFR 104.285, 105.275, or 106.275, or physical, side-by-side accompaniment by a TWIC holder.
 - (a) Physical accompaniment of escorted personnel

Appropriate physical accompaniment exists with 1 TWIC holder escorting no more than 10 non-TWIC holders. In general, requests to increase the number of escorted individuals per TWIC holder will not be approved unless increased security measures are put in place for the duration of the request; also, the approval will be for a limited time only. The request must be submitted to the cognizant COTP in writing and must describe the increased security measures that will be implemented.
 - (b) Monitoring

Protocols for monitoring must enable sufficient observation of the individual with a means to respond if they are observed to be engaging in unauthorized activities or in an unauthorized area. Monitoring can be accomplished in a number of ways, including, but not limited to:

 - 1) Close-circuit television (CCTV) systems can be used to meet this requirement as long as the CCTV systems are monitored and would allow the operator to see in sufficient detail if the non-TWIC holder was moving to an unauthorized area or was engaging in unauthorized activities. The CCTV system must be monitored by a TWIC holder.
 - 2) Intelligent video systems may meet this requirement if the owner or operator can demonstrate equivalency of coverage to the monitored CCTV system to the COTP. Owners or operators should ensure that adequate measures (i.e., security patrols) are in place to respond to unauthorized activities.
 - 3) Other arrangements, using a combination of security patrols or roving watches, automatic intrusion-detection devices or surveillance equipment may be acceptable as long as, when used together, they provide a reasonable assurance that an individual under escort is not engaging in activities other than those for which access was granted.
- (3) Escorting in portions of secure areas that are also restricted areas: escorting must be accomplished by side-by-side accompaniment with a TWIC holder. Side-by-side accompaniment requires continuous physical proximity to and visual contact

with the escorted individual in order to enable the TWIC holder to witness the escorted individual’s actions. In the portions of secure areas that are restricted, each TWIC holder may escort no more than 5 non-TWIC holders, unless otherwise approved by the COTP. In general, requests to increase the number of escorted individuals per TWIC holder will not be approved unless increased security measures are put in place for the duration of the request; also, the approval will be for a limited time only. The request must be submitted to the cognizant COTP in writing and must describe the increased security measures that will be implemented.

- (4) In both cases, there must be sufficient quick response capability to prevent an individual “under escort” from entering an area where he or she has not been authorized to go or from engaging in activities other than those for which escorted access was granted. Sufficient quick response capability can be provided by security guards with communications gear and transportation appropriate to the size of the facility, or watchstanders able to communicate with a roving watch.
- (5) The regulations also require that new hires be accompanied by an individual with a TWIC in secure areas. Accompaniment for this purpose is defined in section 3.3 h. (1) (f) below and is not the same as the general escorting requirements.

	SECURE AREAS THAT ARE NOT ALSO RESTRICTED AREAS	PORTIONS OF SECURE AREAS THAT ARE RESTRICTED AREAS *
		*AS DEFINED IN FSP OR VSP
TWIC HOLDERS	UNESCORTED	UNESCORTED
LOST, STOLEN OR DAMAGED TWICS SEE 3.3 i (2) BELOW FOR FURTHER INFORMATION	UNESCORTED ACCESS UP TO 7 CONSECUTIVE DAYS	UNESCORTED ACCESS UP TO 7 CONSECUTIVE DAYS
NON-TWIC BUT NEW HIRES SEE 3.3 i (1) BELOW FOR FURTHER INFORMATION	ACCOMPANIED ACCESS	ACCOMPANIED ACCESS
NON-TWIC	ESCORTED – PHYSICAL ACCOMPANIMENT (1 TWIC TO 10 ESCORTED) OR MONITORING	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TWIC TO 5 ESCORTED)
U.S. MARINERS	UNESCORTED ACCESS DURING 18 MONTH TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL AS LISTED IN 3.3 i (3) b)	UNESCORTED ACCESS DURING 18 MONTH TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL AS LISTED IN 3.3 i (3) b)
FOREIGN MARINERS	ESCORTED – PHYSICAL ACCOMPANIMENT (1 TO 10 RATIO) OR MONITORING	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TO 5 RATIO)

d. Employee Notification Requirement

- (1) Facility and vessel owners or operators, under 33 CFR 104.200, 105.200, and 106.200 in the TWIC rule, are required to inform facility and vessel employees of their responsibility to possess a TWIC and what parts of the facility and vessel are secure areas, passenger access areas, employee access areas, and public access areas. The intent of this requirement is for owners or operators to determine which of their employees will need a TWIC and inform those employees in

enough time for them to comply with the requirements. Owners and operators are also encouraged, but not required, to provide this same information to personnel who are not facility or vessel employees, e.g. contractors.

- (2) Notification should assist the employee in determining the following:
 - his/her responsibility to possess a TWIC;
 - if he/she will need unescorted access to a secure area;
 - what parts of the facility or vessel are public, employee, or passenger access areas;
 - when compliance will begin in his/her COTP zone; and
 - locations of enrollment centers where he/she can apply for his/her TWIC.
 - (3) Some acceptable forms of notification include the following examples:
 - Signs posted in common areas
 - Company newsletters
 - Announcements by company officials
 - Company website
 - Inserts in wage and salary statements or other payroll documents
 - (4) There will be permanent enrollment centers established around the country. The period with maximum opportunity for quick service is during the peak enrollment time in the local area, and employees should be encouraged to apply for TWICs during that time. See Enclosure (5) for the enrollment implementation schedule.
- e. Incorporation of the TWIC Procedures into Security Plans
- (1) TWIC procedures do not need to be incorporated into existing facility and vessel security plans until the next regularly scheduled submission, 5 years from the initial plan approval date. While facility and vessel owners or operators do not have to amend their plans with the TWIC requirements, they still must comply with these requirements, as stated in 33 CFR 104.405(b), 105.405(b), and 106.405(b).
 - (2) Facility owners or operators desiring to change their secure area definition must submit an amendment to their FSP. This amendment does not need to include the rest of the TWIC requirements until the next regularly scheduled submission, 5 years from the initial plan approval date. The security plan must still cover the entire facility as originally submitted. The intent of providing this provision is to adjust the secure area to require only those individuals who are engaged in maritime transportation-related activities to possess a TWIC, not to reduce the area over which the FSP applies. For further details on this provision, see section 3.4.
- f. Incorporation of the TWIC into Existing Physical Access Control Systems
- (1) Facilities and vessels may incorporate TWIC into their existing physical access control systems as long as these systems ensure that members gaining unescorted access to secure areas possess a TWIC. Facility or vessel access cards may be used to grant unescorted access to secure areas if associated access control systems match an individual's facility or vessel access card to their valid TWIC upon entry. Owners or operators will need to ensure that their own access control systems are updated to show whether the employee has a TWIC, even when

he/she presents only the vessel or facility-specific card, and there must be a way to cancel or deactivate the vessel or facility-specific card if the TWIC is revoked. For example, a facility employee who possesses a valid TWIC may be registered into the facility's access control database and be issued a facility access card. To gain entry into a secure area, the employee would insert their facility access card into a card reader, which would verify the individual as the rightful holder of the access card. The card reader would then verify the individual as a valid TWIC holder by matching the facility access card to the individual's record in the facility database. The facility database would ensure that the employee's TWIC has not been revoked by comparing its employee records to the TSA TWIC list of invalidated TWICs. **In no situation should employees be issued a vessel or facility-specific card which allows them unescorted access to a secure area without first ensuring that the individual possesses a TWIC.**

- (2) Although not required, owners or operators may implement biometric card readers and systems in order to establish identity and ensure that individuals gaining unescorted access to secure areas possess a valid TWIC. These systems may use biometric identifiers other than the fingerprint template on the TWIC (e.g. iris scan or hand print). This may be done only by associating the TWIC profile on the credential to the profile saved on the local physical access control system since the information on the TWIC cannot be altered. Owners or operators may associate any data that they deem necessary to the TWIC profile on their physical access control system. The only limitation is that no alteration may be made to the TWIC card itself. For systems where an additional biometric is used, a vessel or facility access card may be issued as described in paragraph f.(1) above.
- (3) Even if employees are not using TWICs on a daily basis to gain access to the vessel or facility, they must always have the TWIC in their possession while in a secure area for unannounced Coast Guard spot checks and annual inspections, as well as internal vessel or facility security checks. Having a separate access control system will not exempt employees from having TWICs in their possession. Any individuals found unescorted without TWICs in secure areas will be considered a breach of security, and therefore a violation of the regulations. Owners or operators should consider implementing random checks of TWICs at access points to ensure individuals always have the TWIC on their person. A description of how the TWIC is incorporated into existing physical access control systems should be included in the security plan in its next regularly scheduled submission.

g. Knowledge Requirements for Personnel

(1) Company, Vessel, and Facility Security Officers

The CSO, VSO, or FSO will be knowledgeable in, and shall be able to demonstrate familiarity with, all requirements of the TWIC Program as they relate to his/her vessel or facility, including, but not limited to:

- How TWIC applies to the vessel or facility
- Secure/restricted area locations and requirements

- Locations of and requirements for passenger and employee access areas, if applicable
 - Escorting requirements
 - Integration of the TWIC Program into existing access control systems
 - Resolution of violations (forged or tampered TWICs, security breaches)
 - New hire procedures
 - Access for those individuals who have reported lost, stolen, or damaged cards
 - Requirement to notify employees of the TWIC requirement and secure/public access/passenger access/employee access areas
- (2) Security personnel
- Security personnel will be knowledgeable in, and shall be able to demonstrate familiarity with, all requirements of the TWIC Program as they relate to their position, specifically:
- How TWIC applies to the vessel or facility
 - Recognition of a valid TWIC in accordance with section 3.3a of this NVIC
 - Secure/restricted area locations and requirements
 - Locations of and requirements for passenger and employee access areas, if applicable
 - Escorting requirements
 - Resolution of violations (forged or tampered TWICs, security breaches) [See Enclosure (4)]
 - Access for those individuals who have reported lost, stolen, or damaged cards
- h. Special Provisions for Access Control
- (1) New hires
- This provision is intended to limit the risk presented by an individual who has not undergone a full security threat assessment and has not been issued a TWIC, while balancing the need to enable individuals to begin work as soon as possible. Recognizing that there may be a time lag between when individuals may need to begin work and when they receive a TWIC, this provision enables individuals to work with limited access to secure areas after an interim name-based security check has been completed. This provision is granted at the owner's or operator's discretion and only applies to direct employees. Therefore, owners or operators cannot use this provision for other individuals who require unescorted access to secure areas such as longshoremen, truck drivers (unless hired as direct employees), or contractors.
- If an individual is a newly hired vessel or facility employee who has not yet received a TWIC, the owner or operator may grant the individual accompanied access to secure areas of the vessel or facility. Accompanied access is explained in paragraph f) below. This accompanied access may be granted for a period of up to 30 consecutive calendar days, and may be extended for an additional 30 days by the cognizant COTP if TSA has not yet issued the new hire's TWIC, provided all of the following steps are completed:
- (a) The individual has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process and paying the user fee and is not currently engaged in a waiver or appeal process, and the owner or operator has

the individual sign a statement affirming this. There is no format established for this statement. A form can be developed by the owner or operator if needed.

- (b) The individual can present another identification credential that meets the requirements of § 101.515 of this subchapter.
- (c) There are no other circumstances that would cause reasonable suspicion regarding the individual's ability to obtain a TWIC, and the owner or operator has not been informed by the cognizant COTP that the individual poses a security threat. Examples of these circumstances include known criminal history and known immigration violations. This information can be obtained through job applications, job interviews, or the employer's own background check. The owner or operator need not seek these circumstances out; however, if they are known to the owner or operator, they must not allow the individual to have accompanied access under this provision.
- (d) This section may not be used to grant temporary accompanied access to an individual being hired as a Company, Vessel, or Facility Security Officer or any individual being hired to perform security as a primary duty. These positions have greater security responsibility; therefore, we require that the full security threat assessment be completed before they are granted any form of unescorted access.
- (e) The Security Officer must enter the new hire's personal data and employer contact information listed below into the Coast Guard's Homeport website. Homeport is the Coast Guard's portal for sharing information with the public and security officers. Material that is SSI is shared through a secure part of the website with security personnel only, while public information is shared through a non-secure part of the portal. For the new hire provision only, the FSO, VSO, owner, or operator registered in Homeport may use Homeport to request the status of the name-based security check of their newly hired employees. In order for this status to be posted for the FSO, VSO, owner, or operator to view, the following information must be entered **exactly** as it was entered at the enrollment center:
 - Full name*
 - Date of birth*
 - Social Security number (optional)*
 - Employer point of contact and 24-hour contact information
 - Date of TWIC enrollment

***If the information is not entered exactly as it was at the enrollment center the status of the interim name-based check will not be able to be returned and the new hire entry will need to be repeated. For example, if the first name was given as Michael at the enrollment center but was entered into Homeport as Mike, the status of the interim name-based check will not be returned.**

The FSO, VSO, owner, or operator must wait until a positive clearance is given in Homeport before accompanied access can be given to the individual. The interim name-based check should be completed in 3 days or less after enrollment. One way to speed up the process is for individuals to provide

their Social Security number at the enrollment center; this improves the ability to distinguish between two individuals with the same name. However, submission of the Social Security number is optional. If an individual does not provide his/her Social Security number at the enrollment center, providing it on Homeport will not speed up the process.

- (f) New hires do not need to be escorted as other non-TWIC holders do. However, they must be accompanied in accordance with the following criteria:
- 1) No more than 25% of the vessel or facility employees may be allowed to have access under this provision at one time. If there are fewer than four employees, one new hire is allowed. To compute the number of new hires allowed, multiply the total number of vessel or facility employees by 0.25 and round up to the nearest whole number (integer).
 - 2) All security measures for access control and monitoring from the security plan must be followed. If certain measures are not able to be followed for an extended period of time due to maintenance or repairs (i.e. broken camera, degraded fencing, etc.), alternative arrangements must be made to compensate for the gaps in security created by the lack of these measures.
 - 3) The specific guidance for facilities or vessels is noted below:
 - i. Facilities
 - This provision is only available to new hires who are assigned to work units of no more than 25 employees. A work unit is a subset of the larger organization characterized by its geographical location and the extent of its operations, where employees work closely together on a regular basis. This proximity would facilitate accompaniment of a new hire. For example, a work unit may be a fire department on an oil refinery or a business office on a container facility.
 - No more than 25% of the employees in each work unit may be new hires. See guidance in f)1) above for how to compute allowable number of new hires.
 - The individual may be considered accompanied in his/her assigned work area as long as criteria f)1) and f)2) above are met, he/she is a member of a work unit of no more than 25 people, and no more than 25% of the employees in that work unit are new hires. If the new hire is working in restricted areas, the new hire must also be monitored in accordance with 3.3c.(2)(b).
 - Though not required, facility owners or operators should consider issuing identification for new hires listing the expiration date of the accompanied access under this provision.
 - ii. Vessels
 - The total crew required by the vessel's Certificate of Inspection (COI) may not exceed 10. Vessel crew includes all licensed or documented mariners. Vessel crew does not include the following categories listed on the COI: persons in addition to crew, passengers, and other crewmembers.

- The individual may be considered accompanied in his/her assigned work area and living areas (e.g. berthing areas, mess areas, recreation areas, heads) as long as criteria f1) and f2) above are met. If a new hire is working in a restricted area, he or she must also be monitored in accordance with 3.3c.(2)(b).
- (2) Lost, stolen, or damaged TWICs
- If an individual's TWIC is lost, stolen, or damaged, he/she must report that fact to TSA as required in 49 CFR 1572.21. TSA will revoke the card and it will be listed on the list of revoked cards. TSA will then begin the process of producing a new card, which must be picked up at an enrollment center by the individual. During that period when the TWIC has been reported as lost, stolen, or damaged and a new TWIC is being produced and picked up, the individual may be granted unescorted access to secure areas of the facility or vessel for 7 consecutive calendar days under the following circumstances:
- (a) VSO or FSO verifies that the individual had a TWIC and has previously been granted unescorted access to secure areas of the vessel or facility. This can be done by checking employee lists, records of access, or knowledge of security staff.
 - (b) The individual has reported the TWIC as lost, stolen, or damaged to TSA as required in 49 CFR 1572.21. At this point, there is no procedure for the VSO or FSO to check that the card has been reported as lost, stolen, or damaged. However, given the 7 day limitation, it is in the TWIC-holder's best interest to ensure that his/her new card is reported as lost, stolen, or damaged as soon as possible, to ensure that the new TWIC can be manufactured, shipped, and picked up before the 7 days expire.
 - (c) There are no other suspicious circumstances associated with the individual's claim of loss, theft, or damage. Some examples of suspicious circumstances include repeat claims of loss, theft, or damage, questionable explanations for the loss, or coming to work with the TWIC a day or two after claiming it was lost, stolen, or damaged.
 - d) Because the individual is granted unescorted access under this provision for no longer than 7 consecutive calendar days, he or she should pick up his/her card as soon as he/she is informed by TSA that it is available. For mariners overseas, the TWIC will remain at the enrollment center until the mariner returns to the U.S., and the mariner must visit the enrollment center as soon as possible to pick up their TWIC.
- (3) Access control during the enrollment phase-in period
- Over the course of the 18-month initial enrollment period, all individuals will have an opportunity to apply for a TWIC. However, as enrollment centers will be phased in across the country and compliance dates will be based on COTP zone, the potential exists for individuals in mobile populations to come from an area where enrollment has not begun to an area where compliance has started. Recognizing that mariners are a large population for whom this could be a concern, an allowance has been made to enable them to show an alternate identification to gain unescorted access during the 18-month enrollment period. This may also be a concern for long-haul truckers. However, due to the smaller

population and absence of universal identification for long-haul truckers, no allowance has been made for this population.

a) Long-haul truckers

The long-haul trucking population is estimated to be a very small percentage of the total trucking population accessing secure areas at U.S. ports. Most truckers serving ports are local. No truckers will be exempt; all will be required to show a TWIC for unescorted access according to the compliance dates set for each COTP zone. As a result, long-haul truckers who require unescorted access to secure areas are encouraged to enroll as soon as possible as they will be denied unescorted access in zones with early compliance dates.

b) Merchant mariner access

Because mariners are a large, inherently mobile population, mariners will not be required to possess a TWIC for unescorted access to vessels or facilities during the 18-month enrollment period. This will not create a problem on vessels because vessels are not required to comply until 20 months after the publishing date of this rule. However, during this 18-month period, in order for a mariner to have unescorted access to a facility where TWIC is required, the mariner must present one of the following forms of identification in lieu of a TWIC:

- MMD
- CG License and a picture ID
- CG Standards of Training, Certification and Watchkeeping (STCW) Certificate and a picture ID
- CG COR and a picture ID

Mariners are permitted to escort a non-TWIC holder under this provision. Mariners are encouraged to apply early for a TWIC in order to take advantage of surge capacities at enrollment centers while the maximum number of enrollment centers is available in convenient ports. After [insert date], mariners will need a TWIC for unescorted access to secure areas of vessels and facilities.

i. TWIC Procedures Remain the Same Regardless of MARSEC Level

Due to the fact that every individual is required to use TWIC as a visual identification badge in this rule, no additional TWIC requirements are contemplated for changing MARSEC levels.

j. Area Maritime Security (AMS) Committee Members

As AMS Committee members are likely to have access to SSI material, the regulation requires AMS Committee members who do not already require a TWIC in the course of their work to undergo a name-based security check at no cost to the individual. The name-based security check is not a substitute for the comprehensive TWIC security threat assessment, and AMS Committee members applying for TWICs must still bear the cost of TWIC enrollment and issuance. COTPs will forward the names of the AMS Committee members who do not possess a TWIC to CG-3PCP-2 for clearance prior to sharing SSI with these members.

k. Waivers, Exemptions, and Equivalencies of TWIC Requirements

- (1) MTSA 2002 is clear on the applicability of TWIC. Therefore, the Coast Guard does not anticipate that the TWIC requirements will be unnecessary in light of operating conditions for a particular owner or operator and, as a result, does not anticipate granting waivers of the TWIC requirements. However, the existing waiver provisions in parts 104, 105, and 106 of 33 CFR Subchapter H remain unchanged and vessel and facility owners or operators may request a waiver from any provision in the regulation. Vessel and facility owners or operators should submit requests to Commandant (CG-3PC) in accordance with the procedures described in 33 CFR 104.130, 105.130 or 106.125 respectively and applicable references (e) through (g).
- (2) The only parties who are required to submit amendments are those facilities with a non-marine transportation component that want to change the definition of their secure area. All other owners and operators are not required to submit amendments to approved security plans. Amendments to change definitions for secure areas for other types of facilities and for vessels will not be considered.
- (3) U.S. vessels operating under the waivers provided for under 46 U.S.C. 8103(b)(3)(A) or (B) do not have secure areas and therefore are not required to observe TWIC access control requirements. These waivers allow offshore supply vessels and mobile offshore drilling units (or similar vessels) to employ foreigners as crew when operating from a foreign port or beyond the Outer Continental Shelf. See United States Code for details on these waivers. However, when these vessels are not operating under these waivers (i.e. within the U.S. Outer Continental Shelf and shoreward), they do have secure areas and are required to comply with TWIC requirements. Even when serving on vessels operating under the waivers named above, U.S. credentialed Merchant Mariners will still be required to obtain a TWIC.
- (4) The TWIC regulations do not alter the exemption provisions provided in 33 CFR 104.110 and 105.110. The Coast Guard will not consider exempting additional owners or operators from TWIC requirements.
- (5) Current regulations in 33 CFR 101.130, 104.135, 105.135, and 106.130 allow owners or operators to propose an equivalent to for any measure required by part 104, 105, or 106. Proposed equivalents to TWIC requirements submitted in accordance with 33 CFR 101.130 will be considered on a case-by-case basis and must either meet or exceed the security effectiveness of the TWIC Program. Examples of elements of security effectiveness that equivalencies will be measured against include but are not limited to: the tamper resistant features of the TWIC, the security threat assessment, access control provisions, and management of the list of revoked TWICs. Proposals for equivalencies should be specific and detailed in describing how the program will meet or exceed the elements of the TWIC Program.
- (6) Currently approved Alternative Security Programs remain valid and do not have to be resubmitted. However, plan holders may wish to resubmit their Alternative Security Programs to incorporate TWIC Programs in accordance with 33 CFR 101.120, though this is not required.

3.4 Facility-specific Guidance

- a. Amendment of FSPs to Designate Certain Portions of the Facility as Secure Areas for TWIC
 - (1) TWIC is intended to be applied to individuals who require unescorted access to secure areas of maritime transportation vessels and facilities. It is not necessarily intended to be applied to a portion of a facility that does not have a maritime transportation nexus. Although the TWIC rulemaking does not alter the MTSA-regulated geographic area of a facility, it does permit those facilities with a significant non-marine transportation portion to submit an amendment to their FSP to redefine their secure area to cover only the maritime transportation portion of the facility. The FSP must still cover the facility as originally submitted. The intent of this provision is to limit TWIC applicability to the maritime transportation nexus, not to reduce the area over which your FSP applies. Facilities with a significant industrial non-maritime transportation component may apply to the COTP for a redefinition of secure areas for purposes of TWIC. COTPs will assess the feasibility of the request, taking into account the risk for a transportation security incident from the industrial component. Facilities that may be considered to have a significant non-maritime transportation component include, but are not limited to, refineries, chemical plants, factories, mills, power plants, and smelting operations. Facilities and facility areas that are **not** included in this provision include container yards, tank farms and storage areas with material intended for trans-shipment by all modes of transportation, including pipelines, and passenger terminals.
 - (2) The redefined secure area must have all of the access control measures that are currently required by 33 CFR Subchapter H, including fencing, gates, monitoring, etc., in order to ensure that unauthorized persons do not gain access to the secure area. Plans for how access control will be conducted for the redefined secure area must be included in the amendment to the FSP. All amendments must be submitted to the COTP within 6 months after the date of publication of the TWIC final rule in accordance with 33 CFR 105.415 [insert date]. Vessels and facilities must receive approval for the amended plan or receive a letter from the COTP giving them permission to operate under the amended plan before implementing the amended plan.
- b. Amendment Procedures for Redefining Secure Areas

Procedures for submitting amendments to FSPs remain the same and are detailed in References (a) (33 CFR 105.415) and (e).

3.5 Vessel-specific Guidance

- a) Passenger and Employee Access Areas

Recognizing that passenger vessels will be carrying passengers who will not possess TWICs and that some employees rarely need to use spaces beyond those designated for support of passenger entertainment, this rule established two areas of the vessel for which TWICs do not apply for passenger vessels and ferries. These are passenger access areas and employee access areas. Within these areas, individuals are not

required to possess TWICs to gain unescorted access, because they are not part of the secure area. The rest of the vessel remains a secure area, and all spaces not designated as passenger or employee access areas are a part of the secure area and require a TWIC for unescorted access. Vessel security plans do not need to be amended to use these provisions under this rule. However, if passenger access areas or employee access areas are designated, the owner or operator must maintain a visual representation (e.g. an overlay to the fire exit plan) onboard the vessel with the approved VSP detailing where these areas are located as required by 33CFR104.120(c). Written guidance for the crew and employees should also describe actions necessary should a non-TWIC holder be discovered in an unauthorized area or engaging in unauthorized activities. VSPs should be updated to include these areas with the normal resubmission.

- (1) The passenger access areas are the spaces on the vessel open to passengers, such as dining rooms, seating areas, parking decks, public restrooms, and bars.
- (2) Employee access areas include those areas that support passenger access area activities; such as galleys, storage areas, dressing rooms, and food service areas. Employee access areas may not encompass restricted areas. Employee access areas do not apply to U.S.-flagged cruise ships since employees on cruise ships have greater opportunities to create a TSI based on longer voyage lengths, increased contact with passengers, and longer length of time with access to vessel spaces. Due to this increased risk, employees onboard a U.S.-flagged cruise ship must have a TWIC to gain unescorted access to non-passenger spaces.

b) Vessels not Eligible for Redefinition of Secure Areas

Vessels are not eligible to apply for a redefinition of secure areas at this time. All areas of a vessel are inherently transportation-related and may be used to cause a TSI. Therefore, the entire vessel must be designated a secure area, with the exceptions of the passenger and employee access areas as discussed above.

Table of Contents

Enclosure (4) — Enforcement Guidance

	Page
4.1 Enforcement Strategy.....	41
4.2 Enforcement Implementation.....	41
4.3 Invalid/Fraudulent Cards	41
a) Owner or Operator Actions.....	41
b) Possible Coast Guard Actions.....	42

DRAFT

Enclosure (4) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 07-xx

Enforcement Guidance

4.1 Enforcement Strategy

The Coast Guard will work cooperatively with facilities and vessels to verify compliance with the TWIC program. COTPs are strongly encouraged to enhance compliance through proactive engagement with industry. It is very important that the COTP and vessel and facility inspection teams work together with industry personnel so that meaningful security improvements are made permanent. For vessels and facilities that are making an effort in good faith to implement TWIC and are in substantial compliance no enforcement action or letters of warning may be appropriate if on-the-spot corrections of minor deficiencies are made. For those vessels and facilities that are not in substantial compliance, progressive enforcement tools may be used such as Notice of Violation (NOV) or other civil penalties. For egregious vessel and facility noncompliance, operational restrictions, including shutdown, may be available. COTPs are strongly encouraged to contact the cognizant Staff Judge Advocate for guidance on possible enforcement actions in these cases.

4.2 Enforcement Implementation

While the TWIC requirements impose additional security measures that must be verified, the Coast Guard will incorporate compliance within our current vessel and facility inspection examination policies. The new requirements will be verified by Coast Guard personnel on at least an annual basis in conjunction with required examinations/inspections and periodic spot checks. During TWIC verification, Coast Guard personnel will use handheld card readers to validate that the TWIC held by individuals at the facility or vessel being inspected:

- are not counterfeit
- have valid Public Key Infrastructure (PKI) certificates
- have not been revoked by TSA
- match the biometric template on each card to the fingerprint of the person carrying it.

In order to match the biometric on the card to the person, the Personal Identification Number (PIN) given during issuance will be required. Therefore, **it is vital that TWIC holders remember their PIN.**

The compliance date for vessels will be 20 months after the publishing date of the final rule, [insert date]. The compliance dates for facilities will be based on COTP zone and will be announced in the Federal Register at least 90 days before compliance will begin. Compliance dates for facilities can also be found in Enclosure (5).

4.3 Invalid/Fraudulent Cards

a) Owner or Operator Actions

- 1) If a TWIC is presented at a facility or vessel and it is suspected to be fraudulent, according to the features listed in Enclosure (3.3a), the owner or operator should at a minimum:
 - Prevent the individual from having unescorted access to secure areas of the facility or vessel. Escorted access may be granted at the owner or operator's discretion, however, care should be exercised when granting this access since

possession of a TWIC which is suspected to be fraudulent should be considered a suspicious activity.

- Attempt to check the person's identity by asking for one of the alternate forms of identification described in 33CFR101.515. Carefully inspect this identification for signs of tampering and authenticity. Also request the person's name, address, and contact information and record any information given.
- Call the COTP to inform the duty officer that a TWIC suspected to be fraudulent has been presented, the name on the TWIC and the alternate ID presented, name given (if any), and how the TWIC appears to have been tampered with or the signs that indicated a TWIC which is suspected to be fraudulent. Follow any instructions that the duty officer provides.
- Ask the individual to remain at the access control point until the Coast Guard arrives, if the Coast Guard has indicated that they will be coming to collect the TWIC. **DO NOT MAKE ANY ATTEMPT TO RESTRAIN THE INDIVIDUAL OR INFORM THEM THAT THEY MAY NOT LEAVE.** The ability of the owner or operator to take any such action is dependent on state law. The Coast Guard cannot authorize the owner or operator to exercise law enforcement authority. **ONLY A FEDERAL OFFICIAL MAY CONFISCATE A TWIC FROM AN INDIVIDUAL, EVEN A FRAUDULENT OR TAMPERED TWIC.**
- Possible reasons for failure to match the biometric template include:
 - Forgotten PIN
 - False negative reading between TWIC and reader
 - Card reader error
 - Fraudulent or tampered TWIC
 - Damaged or obscured fingerprint
 - TWIC error
 - Revoked TWIC

2) Suspicious activity

As currently required by 33 CFR 101.305 (a), suspicious activity must be reported to the National Response Center at 1-800-424-8802 or 202-372-2428. Suspicious activities related to TWIC use include, but are not limited to:

- Multiple TWICs suspected to be fraudulent presented by different individuals for access in a short period of time (5-7 days)
- An individual attempting to gain access multiple times with the same TWIC which is suspected to be fraudulent (if it is not taken from them)
- Many different appearances of TWICs which are suspected to be fraudulent – possible indicator that there are multiple sources of fraudulent TWICs in the area.
- A single fraudulent TWIC presented by an individual shall be reported to the COTP but need not be reported as suspicious activity to the National Response Center.

b) Possible Coast Guard Actions

- 1) When contacted, the Coast Guard will advise the owner of operator of the vessel or facility whether an inspector will arrive to investigate the TWIC or not. The Coast Guard may respond to the vessel or facility and make additional attempts, including using handheld readers, to verify the TWIC.

- Coast Guard inspectors will attempt to match the biometric template stored on the TWIC to the fingerprint of the individual presenting the card during inspections/examinations and spot checks.
 - If the individual cannot be matched to the TWIC after 3 attempts, the Coast Guard will seize the TWIC take custody of the suspect TWIC and advise the vessel or facility owner or operator on any additional actions the vessel or facility should take.
- 2) If the Coast Guard will not respond to a particular situation, the vessel or facility owner or operator will be so advised.

DRAFT

Enclosure (5) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 07-xx

Implementation Schedule

The implementation and rollout schedule will be available once the contract has been awarded by TSA and the contractor has established the schedule for enrollment ports. This Enclosure will be updated once the schedule is available and will most likely be a link to the online schedule to allow for easy access to the most current version of the schedule.

DRAFT