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 16700.40
NVIC 03-07

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 03-07 JUL 2 2007

Subj: **GUIDANCE FOR THE IMPLEMENTATION OF THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) 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, 1540, 1570, and 1572
c. NVIC 03-03 Change 1 – Implementation of MTSA Regulations for Facilities
d. NVIC 04-03 Change 2 – Verification of Vessel Security Plans for domestic vessels in accordance with MTSA Regulations and ISPS Code
e. 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 (72 FR 3492) (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) will satisfy the requirement for a biometric credential as mandated by 46 U.S.C. § 70105, which was enacted by the Maritime Transportation Security Act of 2002 (MTSA) and then amended by the Security and Accountability For Every (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) and (b), 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 comply with the new regulations 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):

DISTRIBUTION – SDL No. 147

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B																										
C																										
D																										
E																										
F																										
G																										
H																										

NON-STANDARD DISTRIBUTION:

1) All credentialed U.S. merchant mariners with active credentials (hereafter referred to as mariners). This includes all persons holding a Coast Guard-issued Merchant Mariner License, Merchant Mariner Document, or Certificate of Registry;

2) Anyone allowed unescorted access to secure areas of U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) facilities subject to 33 CFR Parts 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/operators, 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/operators are also encouraged to use this guidance to assist in ensuring that they meet TWIC Program requirements. These include but are 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 implementing the TWIC Program and preparing for annual compliance inspections and spot checks of vessels and facilities.

e. COTPs are encouraged to bring this circular to the attention of maritime 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 can 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 rule, some may choose to do so as allowed by reference (a). The only facilities that are required to submit an amendment to their

[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 regulatory text of 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 license or document). 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 to comply with TWIC and is not specifically addressed in the regulatory text of 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.

FSP are those that have a significant non-maritime transportation portion and voluntarily desire to redefine their secure area.

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 (c), (d), and (e) in the future.

4. BACKGROUND.

   a. 46 U.S.C. § 70105, which was enacted by the MTSA, requires the Secretary of DHS to promulgate regulations to prevent an individual from gaining access to a secure area of a vessel or facility which has a security plan unless he/she is authorized to be in the area and holds a "transportation security card" or he/she is "accompanied by another individual who holds a transportation security card." The law further states who must comply (as listed in Action above), that the individual must be determined not to pose a terrorism security risk, and general requirements for how the terrorism security risk determination must be made. The TWIC regulations were developed from this law.

   b. The TWIC rule, which amended the regulations found in references (a) and (b), 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 rule and reference (b) includes the TSA portions of the rule.

   c. The TWIC Program aims to ensure that only persons who successfully undergo 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 will be required to choose and remember a Personal Identification Number (PIN). TWIC holders will be asked by a vessel or facility owner/operator to produce the TWIC before being granted unescorted access or during Coast Guard inspections or spot checks. 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. While an owner/operator is not currently required to verify if a TWIC is revoked, if he/she has knowledge that a TWIC is revoked, that TWIC cannot be accepted for unescorted access. TSA has designed the TWIC process to maintain strict privacy controls so that a holder's biographic and biometric information are securely protected.

   d. The Coast Guard and TSA are currently conducting screening of facility employees and longshoremen, known as the interim vetting program, pursuant to a Federal Register Notice on April 28, 2006. For this program, facility operators and longshore unions have submitted names of employees and long-term contractors for vetting through select Federal databases. We anticipate that this requirement will continue to be in force until TWIC initial enrollment has been completed. A Federal Register notice will be published when this program is cancelled.

5. DISCUSSION.

a. Vessels and facilities must be in compliance with the TWIC regulations as discussed in paragraphs 6 b., c., and d. below, but in no case later than September 25, 2008, , which is 20 months after the publication 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, the expiration date will be checked, 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 (e.g. has not been revoked) and to match the individual to the biometric template stored on the card.

c. Possession of a TWIC is required for an individual to be eligible for unescorted access to secure areas of vessels and facilities. The term "secure area" is defined as "the area over which the owner/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 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 footprint as described in their currently approved facility security plan, with the exception of public access areas and those facilities with significant non-maritime transportation portions who submit an amendment to redefine their secure area. All of these provisions are explained in Enclosure (3) (section 3.3 b).

d. An individual with a TWIC who is authorized to be in a secure area by the vessel or facility owner/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 accompanied, as opposed to escorted, as explained in Enclosure (3) (section 3.3 h (3)(d)).

e. Company, vessel, and facility security officers and company, vessel, and facility personnel responsible for security duties are required by regulation to obtain a TWIC. We expect that individuals who frequently access secure areas in the course of their employment will obtain TWICs. These populations include: non-credentialed mariners in vessel crew; longshoremen; drayage truckers; facility employees who work in a secure area; truckers bringing cargo onto a facility or picking up cargo at a facility; surveyors; agents; chandlers; port chaplains; and other maritime professionals. This list is not exhaustive and other populations may be included. Casual laborers who frequently access secure areas in the course of their employment would also be expected to obtain a TWIC. Casual laborers who only occasionally access secure areas and

therefore do not have a TWIC would need to be escorted. Additional details are provided in Enclosure (2) (section 2.1).

f. Escort requirements differ within secure areas depending on whether the area is also 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 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. Additional details are provided in Enclosure (3) (section 3.3 c).

g. 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, with an additional 30 days at COTP discretion. Owners/operators must complete additional steps before new hires may be granted accompanied access. Additional details on this provision are provided in Enclosure (3) (section 3.3 h(1)).

h. 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 be eligible for 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) (section 3.5 b).

i. The TWIC may be incorporated into existing physical access control systems. If this is done individuals must still always have their TWIC in their possession or readily available and the existing systems should be updated so that they deny access when the TWIC expires or if the TWIC holder no longer requires unescorted access to a secure area. Additional details on this provision are provided in Enclosure (3) (section3.3 f).

j. Amplification of the knowledge requirements for Company, Vessel, and Facility Security Officers, for personnel with security duties, and for all other personnel is provided in Enclosure (3) (section 3.3 g).

k. If an individual's TWIC is lost, stolen, or damaged, unescorted access to secure areas may be granted for seven consecutive calendar days while the individual awaits a replacement. Additional steps must be completed by both the individual and the Company Security Officer (CSO), Vessel Security Officer (VSO), or Facility Security Officer (FSO). These additional details are provided in Enclosure (3) (section 3.3 h (2)).

l. All vessel personnel 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 to be eligible for unescorted access to secure areas by September 25, 2008. Until this date, all mariners will be eligible for 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) (section 3.3 h (3)).

m. Area Maritime Security (AMS) Committee members are not required to obtain a TWIC. However, if they have access to Sensitive Security Information (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) (section 3.3 i).

n. Owners or operators of facilities containing both a maritime transportation portion and a non-maritime 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 on this option are provided in Enclosure (3) (section 3.4).

o. 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. Enrollment and issuance of the TWIC will be carried out by TSA. Enforcement of the TWIC as an access control measure in the maritime sector will be carried out by the Coast Guard. TWIC enrollment will begin in selected ports and will expand nationwide to provide ample opportunity for individuals to apply for and receive their TWIC. The requirement to use the TWIC as an access control credential will be based on location and type of operation as explained below.

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. In no case will the compliance date be later than September 25, 2008 in any COTP zone.

(4) A rollout plan, describing implementation across all COTP zones, 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 for OCS facilities is no later than September 25, 2008. Federal Register notices for enrollment dates will be published for port areas as described above. OCS facility employees requiring TWICs should apply while centers are open in their local areas, despite the later compliance date.

d. Compliance with this rule for vessels is no later than September 25, 2008. On this date, all individuals must present a TWIC to be eligible for unescorted access to secure areas of vessels.

e. Also by September 25, 2008, all mariners will be required to hold a TWIC in order for their license, MMD, COR, or STCW endorsement to remain valid. Until then, if the vessel or facility has started TWIC compliance and enforcement, mariners may present an alternate identification to be eligible for unescorted access to secure areas of the vessel or facility. Alternative mariner identifications are listed along with additional details in Enclosure (3) (section 3.3 h (3)).

f. 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)].

g. Enclosure (1) is a TSA flowchart of the TWIC enrollment and issuance process.

h. Enclosure (2) is a TSA publication that provides more detail and guidance for the enrollment and issuance process.

i. Enclosure (3) provides guidance on facility and vessel implementation.

j. Enclosure (4) provides guidance on enforcement of the TWIC requirements.

k. Enclosure (5) is the implementation schedule for enrollment nationwide.

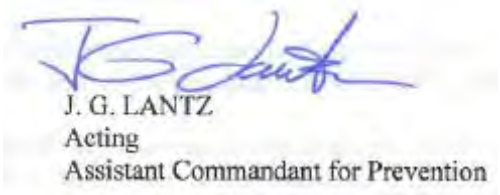
7. INFORMATION SECURITY. TWIC credentials and associated databases contain sensitive personal information that, if released to the general public or improperly accessed or used by personnel executing their official duties, could compromise the privacy of an individual. This information shall be protected 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 regulation. 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 in the next change to this circular.

Suggestions for improvement of this circular should be submitted in writing to Commandant (CG-3PC).

10. FORMS AND REPORTS. None.



J. G. LANTZ
Acting
Assistant Commandant for Prevention

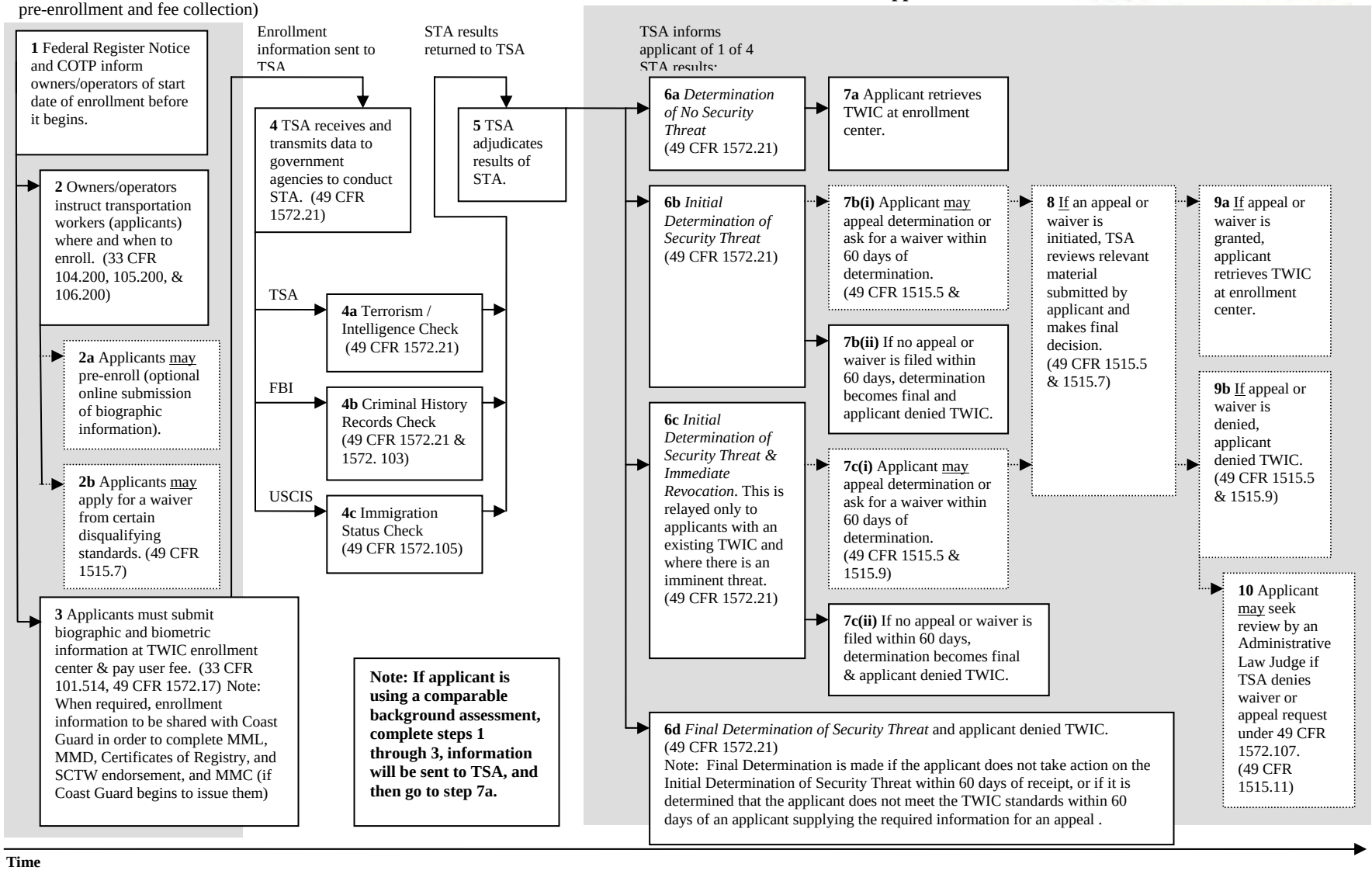
Encl: (1) TWIC Enrollment and Issuance Process Flowchart
(2) Enrollment and Issuance Process Description
(3) TWIC Program Implementation for Vessels and Facilities
(4) Enforcement Guidance
(5) Implementation Schedule

TWIC Enrollment and Issuance Process Flowchart

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

Transportation Security Administration

This diagram depicts the process of applying for and obtaining a TWIC. More information is available by viewing the references to the Code of Federal Regulations (CFR) sections included in each box. Further clarification is also provided in Enclosure (2) of this Navigation and Vessel Inspection Circular. Other information is available at http://www.tsa.gov/twic and http://homeport.uscg.mil.



This page intentionally left blank

Table of Contents

This page intentionally left blank

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

Transportation Security Administration

Enrollment and Issuance Process Description

2.1 Who must get a TWIC?

All mariners and individuals who will need unescorted access to secure areas of a vessel or facility will need to obtain a TWIC. Vessel or facility owners/operators determine who will need unescorted access to the secure area(s) of their vessel or facility. Owners/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 be granted by the vessel or facility owner/operator**. We expect that the following communities will need frequent access to secure areas in the course of their employment and will obtain 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.
- Facility employees if working in a secure area.
- Truckers bringing cargo onto a facility or picking up cargo at a facility.
- Surveyors.
- Agents.
- Chandlers.
- Port Chaplains.
- Casual laborers who frequently access secure areas.
- Other maritime professionals.

Company, vessel, and facility security officers and company, vessel, and facility personnel responsible for security duties are required by regulation to obtain a TWIC. Personnel responsible for security duties include individuals whose fundamental responsibilities focus on security of the vessel or facility. These positions include security guards, baggage screeners, and persons making access control decisions as a primary duty. While recognizing that security is everyone's duty, it does not include individuals who perform security duties as an occasional task or as a collateral duty.

2.2 Who can apply for a TWIC?

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

a. A national (includes citizen) 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;
   (7) TN North American Free Trade Agreement;
   (8) C-1/D, Crew Visas.

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, or
- 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 is wanted for any crime, under indictment for one of the disqualifying felonies listed in 49 CFR 1572.103, or has been convicted or incarcerated for those disqualifying felonies 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 TSA determines that 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. Typical reasons for an appeal would be 'my conviction was later expunged,' or 'you have the wrong John Smith.'

What if I know I do not meet the qualification standards?

- 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 of enrollment, the applicant should annotate by initialing they are applying for a waiver on the 'TWIC Application Disclosure Form.' 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 as well.

2.6 TWIC Enrollment

Employee Notification Requirement

- Facility and vessel owners/operators, under 33 CFR 104.200, 105.200, and 106.200, 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/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/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 secure, 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; and
  - 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, and there will be a link provided on the Coast Guard's Homeport site to this information as well (http://homeport.uscg.mil).
- 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) (section 3.2) 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 over a secure site; 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. This list is also available on the TSA/TWIC website, but consolidating it with the pre-enrollment documents should make the process more efficient applicants.
  - Allows the applicant to become familiar with the disclosure form, which should be signed at the beginning of the enrollment process, in the presence of the Trusted Agent at the enrollment center.
  - Provides the enrollment site locations and hours of operation. This list is also available on the TSA/TWIC website, but consolidating it with the pre-enrollment documents should make the process more efficient applicants.
  - 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 access to the World Wide Web. 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.
- A unique registration number will be assigned to an applicant when they pre-enroll. At the end of the pre-enrollment process, the applicant will be instructed to print out a page with their registration number (it is displayed as a bar code) or to write down their registration number if they do not have access to a printer. This page will also include information on the applicant's enrollment appointment, if selected. Note: other methods will exist for retrieving the pre-enrollment data if an individual does not have their registration number with them at the time of enrollment.

(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. As stated above, if the applicant pre-enrolls, they are asked to bring their registration number by either printing out the page identifying it during the pre-enrollment process or by writing it down.
- 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, but is also listed here. Applicants provide either one document from List A or two documents from List B, one of which must be a government-issued photo ID.

  List A
  - Unexpired Passport
  - Unexpired Permanent Resident card or Unexpired Alien Registration Receipt Card with photograph
  - Unexpired Foreign passport with one of the following:
    - I-551 Stamp
    - Attached INS Form I-94 indicating unexpired employment authorization
    - Unexpired employment Authorization Document (I-766)
    - Unexpired Employment Authorization Card (INS-688B)
    - Unexpired Visas: E-1, E-2, E-3, H-1B, H-1B1, L-1, O-1, TN, M-1, C-1/D
  - Unexpired Free and Secure Trade (FAST) Card
  - Unexpired Merchant Mariner Document (MMD)

  List B (need two and one must be a government-issued photo ID)
  - U.S. Certificate of Citizenship (N-560,561)
  - U.S. Certificate of Naturalization (N-550 or 570)
  - Driver's license or ID card issued by a state or outlying possession of the United States

  - Original or certified copy of birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal
  - Voter's Registration Card
  - Consular Report of Birth Abroad
  - U. S. Military ID or Retired Military ID
  - Military Dependent's Card
  - Expired U.S. Passport
  - Native American Tribal Document
  - U.S. Social Security Card
  - U.S. Citizen Card I-197
  - U.S. Military Discharge Papers DD-214
  - Department of Transportation (DOT) Medical Card
  - Civil Marriage Certificate
  - Unexpired U.S. Merchant Mariner's License
- Applicants must sign the TWIC Application Disclosure Form at the enrollment center; minors can sign without parental/guardian consent.
- 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. TSA will also provide digital photographs, fingerprints, and FBI numbers to the Coast Guard for use in evaluation of applicants. Sharing this information between TSA and USCG is expected to occur at the time that TWICs are required for all credentialed merchant mariners.
- All applicants will receive a TWIC Application Disclosure Form which must be signed in the presence of the enrollment personnel under contract to TSA at the beginning of the enrollment process. The enrollment personnel are known as "Trusted Agents" because they must successfully complete a rigorous threat assessment and extensive training on the enrollment process. 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 disclosure form is provided with the application on-line for them to familiarize themselves.
- 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. If an applicant refuses to sit for a photograph, enrollment will not proceed. Fingerprinting will consist of 10 fingers unless the applicant has lost or seriously injured his or her fingers. For applicants who cannot provide any fingerprints, TSA will use alternate procedures approved by

the FBI to conduct the security threat assessment. (After card activation, these applicants will confirm their identity when required by using their photograph and PIN.) 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 should so state on the disclosure form. Individuals who fail to notify TSA of disqualifying events are subject to immediate revocation (if they already possess a TWIC) and civil penalties, if TSA so chooses. In addition, if an applicant is not truthful on the application, criminal sanctions may apply.
- Information on the TSA website www.tsa.gov/twic will provide guidance on the process. Additionally, section 2.8 (Privacy and Information Security) identifies program controls in place to protect an applicant's privacy.

(3) Fee Collection

- Applicants will pay a fee in accordance with the following table*:*

Category	Fee
Individuals requiring a security threat assessment	$137.25
Individuals not requiring a security threat assessment (e.g. 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)	$105.25
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 (HME), FAST card, merchant mariner's document (MMD), or merchant mariner license) may pay a reduced TWIC fee because they do not need another threat assessment. In order to do so, they must present their HME, FAST card, MMD, or merchant mariner license at the time of enrollment. The TWIC expiration date for HME, FAST, MMD, and merchant mariner license holders will be five years from the date those credentials were issued.
- Note: It is most beneficial for applicants who will use a comparable threat assessment and pay the reduced fee to do so within 14 months of receiving the comparable threat assessment (HME, FAST, MMD, license, etc.). After 14 months,

it is more cost effective to pay the full fee for TSA to complete the security threat assessment and issue a TWIC with an expiration date 5 years from the date of 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 the 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 (this notification would be sent to the National Maritime Center so that they would not be issued a mariner document/license/credential).
- 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.
- 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. Additionally, TSA will notify law enforcement when appropriate.

(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 6-digit personal identification number (PIN) that is stored on the credential. The PIN can subsequently be used 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. **The PIN will be used during Coast Guard inspections and spot checks to match the biometric on the TWIC to an individual and therefore it is extremely important that it be remembered!** Individuals should take care to choose a PIN that can be remembered even if used infrequently.
- 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 when 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. TSA will revoke the credential based on any subsequent disqualifying event (refer to regulation). In these cases, the TWIC holder will be notified via mail and if information exists indicating that the person is an imminent threat, then this will be shared with appropriate parties (e.g. employer, facility or vessel owner/operator, COTP, or law enforcement.)
- Additionally, individuals 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 a brief explanation and instructions on how to apply for an appeal or waiver.
- *Waivers*
  - TSA has designed a waiver process that is straightforward. Applicants need not be represented by counsel nor be conversant with legal terms and processes. TSA accepts hand-written applications, so the applicant does not need to have a computer or typewriter to apply for a waiver.
  - Applicants must annotate the enrollment disclosure form that they will be applying for a waiver 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.) will contain 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/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/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). Information on the ALJ process is available in section 49 CFR 1515.11 of the TWIC final rule.

- *Appeals*
  - The appeal process is available to all applicants if they believe TSA has not applied the disqualifying 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 must initiate 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 ALJ.

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 appropriate government agencies 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 Help Desk

- A toll-free TWIC help desk (*1-866-DHS-TWIC)* 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 help desk 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 before needing to have the PIN reset), etc. Assistance 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.
- Both TSA (571-227-4545) and the Coast Guard (877-687-2243) will have a help desk in order to address calls that do not come directly through 1-866-DHS-TWIC. These help desks will coordinate/communicate as appropriate.

2.10 TWIC Renewal

- Generally, TWICs remain valid for five years, unless renewed before the five-year expiration date, deactivated, or revoked. 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, COR, or merchant mariner license), the TWIC will expire five years from the date of the comparable threat assessment and credential issuance.
- 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 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 help desk immediately at 1-866-DHS-TWIC.
- After the applicant reports the card as lost, stolen, or damaged, the help desk 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 for pick up.
- 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. This list of revoked cards (the 'hotlist') will be available on the TWIC portal to appropriate individuals within the maritime community (VSO, FSO, COTP) in order to monitor access to secure areas. Once the replacement TWIC

arrives at the enrollment center, the applicant will pick it up and pay the card replacement fee of $36. (An increase to $60 has been proposed.)

- The replacement card will have the same expiration date as the original.

Table of Contents

This page intentionally left blank

TWIC Program Implementation for Vessels and Facilities

3.1 TWIC Applicability

3.1 a. Vessels

(1) The TWIC 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 (see 33 CFR 101.105) and therefore are not required to observe TWIC requirements. However, all other MTSA requirements remain unchanged. This waiver allows offshore supply vessels and mobile offshore drilling units (or similar vessels) to employ foreign 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 (e.g., 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 subject to 33 CFR Part 104 will be required to comply with the TWIC requirements regardless of location.

(3) TWIC requirements do not apply to foreign-flagged vessels subject to 33 CFR Part 104.

(4) Warships, naval auxiliaries (USNS vessels), or other vessels owned or operated by the U.S. government and used only on government non-commercial service are exempt from the requirements of 33 CFR Part 104, including TWIC requirements. If a vessel that would not normally be subject to 33 CFR Part 104 has voluntarily complied and has an approved VSP, they must comply with the TWIC requirements in 33 CFR Part 104. Mariners who hold a License, MMD, and/or COR and serve aboard a vessel above are still required to obtain a TWIC in accordance with 46 CFR 10.203.

(5) The TWIC requirements do not apply to mariners (credentialed or uncredentialed) on facilities working immediately adjacent to the vessels they are employed aboard while in the conduct of vessel activities. This allows mariners limited access to the area immediately adjacent to their vessels to conduct operations in support of the vessel (e.g. attach shore ties, perform maintenance, read load lines, load stores, etc.) without escort. 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 obtain a TWIC.

(6) As the majority of foreign mariners are not eligible to obtain a TWIC, they will not be entitled to unescorted access, except in the limited area immediately adjacent to their vessels as stated above. They will still need to present a form of personal identification that complies with 33 CFR 101.515 to seek entry to the facility. The Coast Guard considers the following identity documents as meeting the requirements for “personal identification”:

a) Passports
b) Seaman’s books
c) Seafarer Identity Documents issued in accordance with ILO-147
d) STCW certificates

3.1 a.(6) e) Drivers licenses
f) Other photo identification meeting the requirements of 33 CFR 101.515 provided by the vessel owner/operator

3.1 b. Facilities

(1) The TWIC access control requirements apply to all facilities subject to 33 CFR Parts 105 and 106.
(2) Public access facilities which are exempt from the access control provisions in 33 CFR Part 105 are not required to implement any part of the TWIC Program.
(3) Facilities which have intermittent operations currently approved in their FSPs, and have approved periods when personal identification is not checked, may exclude TWIC access control procedures during those periods.

3.1 c. Exempted populations

The following populations do not require a TWIC for unescorted access: Federal officials, State and local law enforcement officials, and emergency responders when responding to an emergency situation.

(1) Federal officials, which includes any employee of the Federal government, may only gain unescorted access during the course of their official duties. They must present their current agency credentials for visual inspection, except in case of emergencies or other exigent circumstances. Federal government contractors with Federal government-issued HSPD-12 compliant credentials may be considered Federal officials. Federal government contractors without Federal government-issued HSPD-12 compliant credentials are not included in this exemption.
(2) State and local law enforcement officials may use this exemption in the course of their official duties. An off-duty State or local law enforcement official employed as a security guard is not acting in the course of their official duties. However, State and local law enforcement officials who require unescorted access to a secure area as part of off-duty employment may obtain a TWIC.
(3) Emergency responders, which is interpreted as those emergency responders employed by a government agency and any medical personnel, may gain unescorted access only when responding to an emergency situation. State and local emergency responders that are also law enforcement officials fall under the exemption in 3.1 c. (2) above. Non-State and local emergency responders (e.g. oil spill removal organization employees) will need a TWIC.

3.2 TWIC Implementation Schedule

3.2 a. Enrollment

TWIC implementation will begin with the establishment of TWIC enrollment centers. These are contractor-operated locations that enroll individuals 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, on September 25, 2008 (see 33 CFR 104.115, 105.115, and 106.110). Enrollment center locations and staff will then be reduced as appropriate to manage the enrollment of new individuals entering the maritime-related workforce, replacements of lost, stolen, or damaged TWICs, and TWIC renewals. Enrollment centers will remain in locations convenient to the centers of regulated port facility and vessel activity after the phase-in period.

A current schedule of enrollment center phase-in will be posted online at www.tsa.gov/twic and http://homeport.uscg.mil to facilitate timely communication of updates and changes. The schedule of the rollout of enrollment centers nationally may change as rollout progresses, so individuals need to check this website in order to get up-to-date information. See Enclosure (5) for more information.

3.2 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 the date 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) OCS Facilities

In keeping with current 33 CFR Part 106 compliance practice, TWIC compliance for OCS facilities will be managed by Coast Guard District instead of COTP zone as indicated in the regulation. The compliance date for all OCS facilities will be September 25, 2008.

(3) 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 September 25, 2008. However, owners and operators of vessels that operate exclusively within a single COTP zone are encouraged to 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 will be eligible for unescorted access by showing an alternative identification. See paragraph 3.3 h. (3) (b) for additional information on mariner unescorted access through regulated facilities during the TWIC phase-in period.

(4) Mariners

Mariners are required to obtain a TWIC by September 25, 2008, in order for the MMD, license, COR, and STCW endorsement to remain valid. Failure to obtain a TWIC may result in suspension or revocation of the mariner's credential under 46 U.S.C. 7702 and 7703.

Type of operation	Compliance Date
Vessels (33 CFR 104)	September 25, 2008
Facilities (33 CFR 105)	by COTP zone – date published in Federal Register
OCS Facilities (33 CFR 106)	September 25, 2008
Merchant Mariners	September 25, 2008

Table 1 – Compliance dates based on type of operation

3.3 Vessel and Facility Guidance

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

(1) The TWIC will be employed as a visual identification badge for an individual to be eligible for 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. Verification of the TWIC must take place before the individual is granted unescorted access to secure areas, but does not need to take place every time the individual is granted unescorted access if the individual is moving from one secure area to another.

> **EXAMPLE:** An individual is moving from a secure area on a facility to a secure area on a ship loading stores. In this case, the TWIC would be verified the first time the individual is granted unescorted access to the secure area on the vessel and then the individual could be allowed to move freely on and off the vessel.

> **EXAMPLE:** An individual is a crewmember onboard a passenger vessel. In this case he/she may be granted unescorted access to secure areas after the TWIC has been verified at the access control point. These individuals may move between secure areas and passenger and employee access areas without having to verify the TWIC each time.

Otherwise, this should not be used for individuals leaving the secure area to a non-secure area.

> **EXAMPLE:** An individual is leaving the facility for lunch. In this case, the TWIC would need to be verified upon the individual's return.

In all cases, the TWIC must be verified at a minimum of at least once a day, unless underway on a vessel where the entire vessel is a secure area. Owners/operators can require verification more frequently than once per day if desired. If TWIC is incorporated into existing physical access control systems, verification must occur before the company card is issued. The company issued card must be verified before granting unescorted access to a secure area. Random checks should be incorporated to ensure that individuals maintain the TWIC on

their person or in close proximity to their work station. Incorporation into physical access control systems is described further in section 3.3 f. below.

3.3 a.(2) **The regulation does not currently require owners/operators to employ readers to verify the electronic features of the TWIC at this time.** If owners/operators choose this additional security measure, TWIC holders must submit their TWIC for inspection when requested by the owner/operator while in a secure area or when requesting unescorted access to a secure area. This will require the TWIC holder to enter his/her PIN.

(3) As with other responsibilities in 33 CFR Subchapter H, facilities may accept the responsibility for verification of TWICs for vessels moored on their property (or vessels may accept responsibility for the facilities). If this is done, specific responsibilities and procedures must be detailed in a Declaration of Security and signed by both parties.

(4) The TWIC may be verified by security personnel as described for verification of personal identification in the currently approved VSP or FSP. These security personnel shall possess a TWIC.

(5) Individuals granted unescorted access should carry the TWIC on their person when they are in a secure area and the TWIC must be available for inspection if requested by owners/operators, security personnel, or Coast Guard inspectors. However, if owners/operators determine that having their personnel physically maintain the TWIC on their person is impractical, the credentials may be secured in a convenient location where they can be retrieved and presented within a reasonable amount of time for inspection or examination. Ten minutes or less is considered a reasonable amount of time. The TWIC does not need to be worn on clothing, but owners/operators may choose to require personnel to visibly display their TWICs while on a facility or aboard a vessel.

> **EXAMPLE:** A vessel owner/operator may collect and store all crew member TWICs in a secure location in the pilot house of an underway vessel, or crewmembers may secure their TWIC in their cabins while working onboard a vessel.

(6) 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 knowledgeable in 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 a 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 VSP or FSP. However, if these methodologies are used, they should be capable of readily identifying the security features of the TWIC. If the alternative verification methodologies are not capable of verifying all the security features, random physical visual checks of TWICs should be incorporated specifically to verify those features which may be more difficult to see on camera systems.

3.3 a.(7) 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. See http:\\homeport.uscg.mil for images of the TWIC and a description of the security features.

3.3 b. Secure Areas

(1) A key element of the TWIC Program is the definition of the secure area. A secure area is defined as "the area over which an owner/operator has implemented security measures for access control." For vessels and OCS facilities, the secure area encompasses the entirety of a vessel or OCS facility, with the exception of passenger or employee access areas for vessels (see discussion in section 3.5). For facilities, 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, with the exception of paragraph 3.3 b (3) below. The secure area is bound by the fence line, gates, waterfront, and other means that provide access control to the area. The secure area is the area regulated by 33 CFR Part 105 and is encompassed by the currently approved security plan.

(2) The terms "secure area" and "restricted area" do not mean the same thing. The restricted area is 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) 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). Restricted areas of a vessel or facility present a heightened opportunity for a TSI. By virtue of the fact that the secure area encompasses the entire facility or vessel, restricted areas fall within this perimeter.

(3) Facilities with a significant non-maritime transportation portion may submit an amendment to their FSP to request to redefine their secure area to include only the maritime transportation portion of the facility. During this redefinition process, some restricted areas may be eligible for placement outside of the new secure area depending on their type. (see discussion in section 3.4)

(4) Secure areas, employee access areas, passenger access areas, and public access areas must be clearly marked on vessels and facilities in accordance with 104.200 and 105.200. Secure areas are not required to be marked on OCS facilities due to the fact that the entire facility is a secure area. Restricted areas must already be clearly marked with specific wording in accordance with 104.270, 105.260, and 106.265.

(5) Examples of secure areas include, but are not limited to the following:

> **EXAMPLE**: A facility consists of a pier, storage tanks, and truck cargo loading rack. The entire area is a secure area. It is not eligible for a redefinition of the secure area because it does not have a significant non-

maritime transportation portion and therefore, the entire footprint covered by the FSP is a secure area, including the loading rack. (See section 3.4 for details on redefinition of secure areas)

EXAMPLE: A passenger terminal has an approved public access area. The passenger terminal outer perimeter would be the circumference of the secure area and the public access area would create a path through the secure area where passengers could travel unescorted from the perimeter to the vessel. If employees needed to leave the public access area and enter a secure area, they would need a TWIC or be escorted. If passengers needed to leave the public access area and enter a secure area, they would need to be escorted.

EXAMPLE: A passenger vessel (other than cruise ship) has designated employee access areas and passenger access areas. The vessel would have passenger access areas starting at the gangway and encompassing the seating areas, dining room, casino, viewing decks, and restrooms. Employee access areas would abut the passenger access areas and include the galley and other food preparation areas, entertainer preparation and changing areas, employee lounges, bar areas, and storage areas. All remaining areas of the vessel would be secure areas including all restricted areas such as the bridge and the engine room.

3.3 b.(6) Figures below are representations of secure areas on the following types of facilities and vessels:

- Figure 1 - Cargo vessel
- Figure 2 - Passenger vessel
- Figure 3 - Marine terminal, wholly transportation related
- Figure 4 - Marine terminal, containing non-maritime transportation portions after COTP approval of FSP amendment redefining secure area

These representations are illustrations 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.

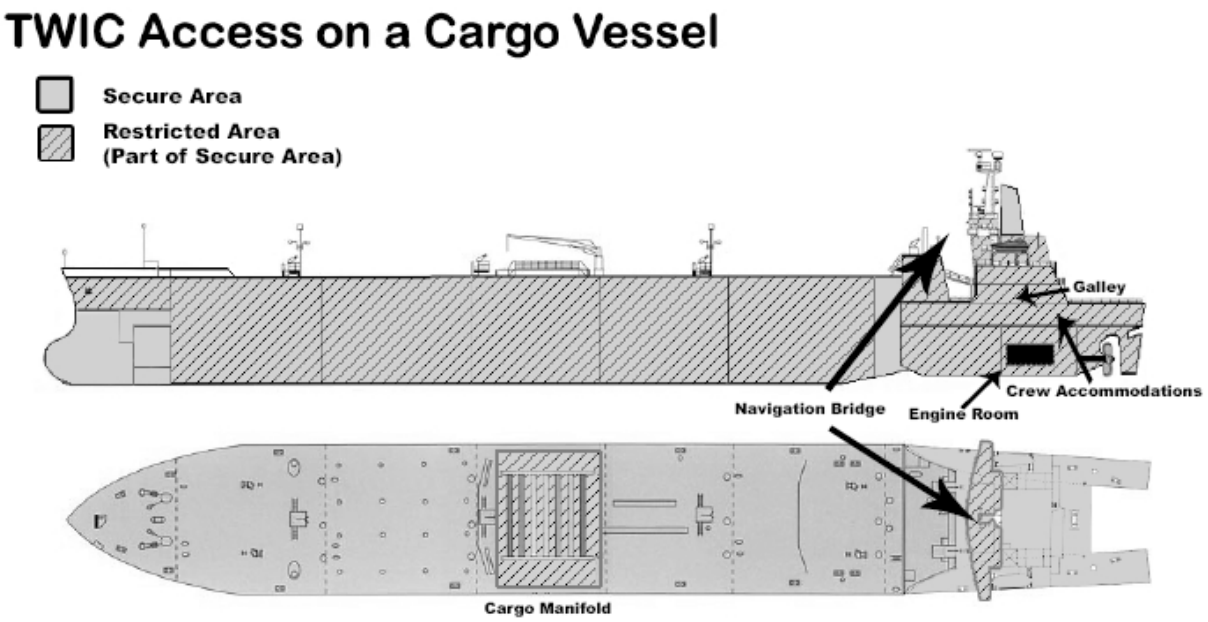


Figure 1 – Cargo vessel

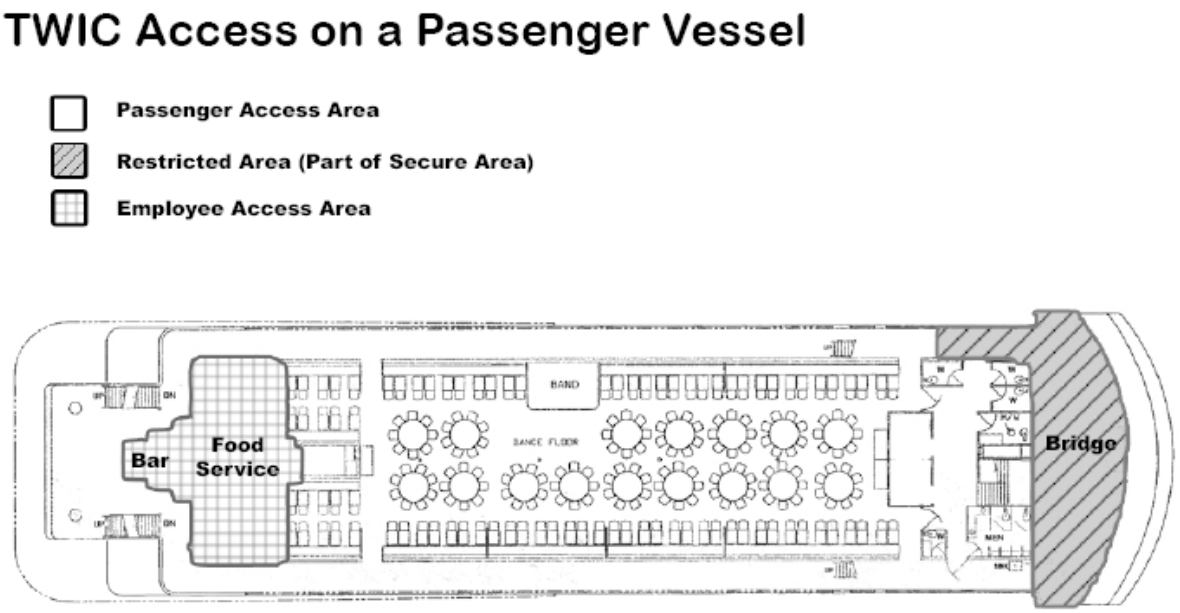


Figure 2 - Passenger vessel

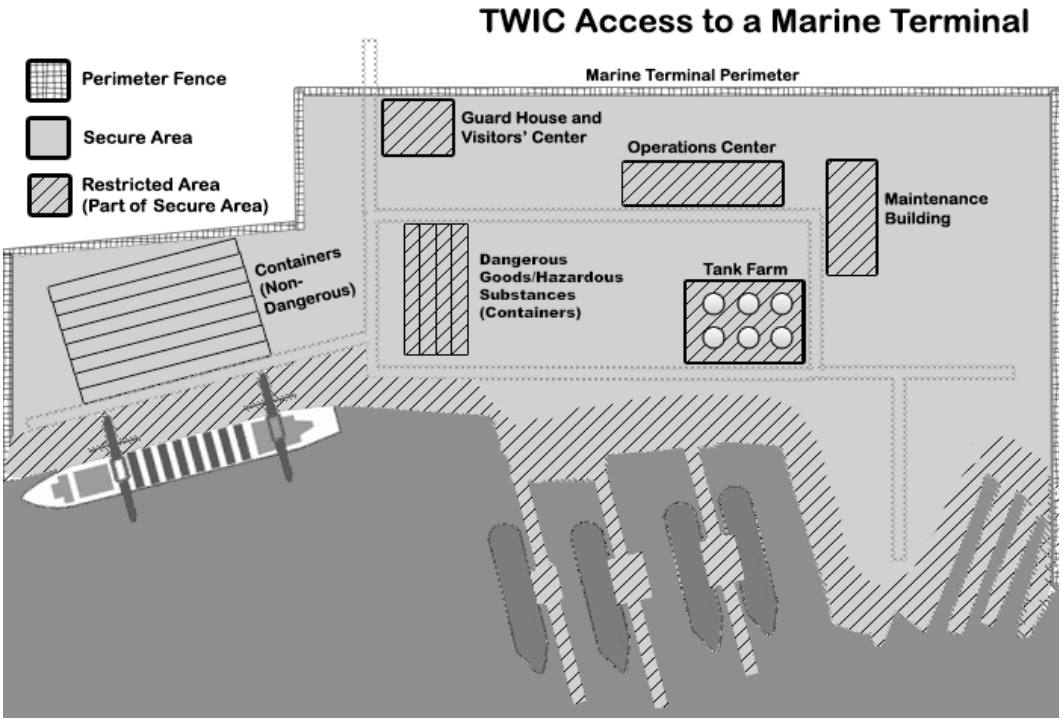


Figure 3 - Marine terminal, wholly transportation related

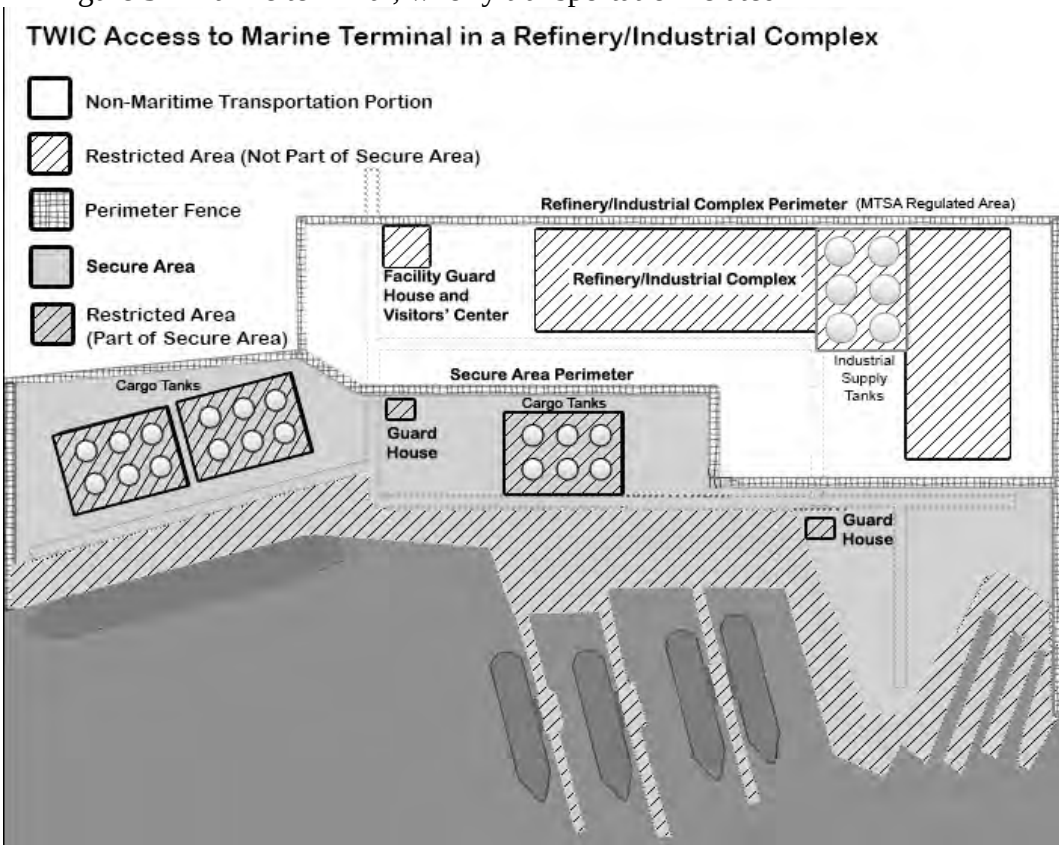


Figure 4 - Marine terminal, some non-maritime transportation portions after COTP approval of FSP amendment redefining secure area

3.3 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 if granted access to a secure area by the owner/operator. The owner/operator is responsible for determining how escorting will be carried out in accordance with this guidance. We expect that individuals who frequently access secure areas in the course of their employment will obtain TWICs and therefore will be eligible for unescorted access. 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 (methodologies 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 one TWIC holder escorting no more than 10 non-TWIC holders. Owners/operators that choose a different physical accompaniment criteria will likely receive increased scrutiny from COTPs. Owners/operators are strongly encouraged to discuss deviations from this number with their COTP.

> **EXAMPLE**: A longshore foreman with a TWIC is requesting to escort 10 longshoremen. The owner/operator should not approve this request. The Coast Guard does not believe that a longshore foreman can serve as an escort to 10 longshoremen, given the requirement that an escort be able to observe whether any of the 10 escorted individuals is engaging in activities other than those for which escorted access was granted. By the nature of their occupation, longshoremen are expected to perform a variety of tasks which are likely to take them out of the line of sight of a foreman/escort. Therefore one person would not be able to meet the escorting requirements for 10 longshoremen. This example would also apply in restricted areas if the foreman was requesting to escort five longshoremen (see escorting guidance for secure areas that are also restricted areas below).
>
> **EXAMPLE**: A truck driver is requesting to escort a non-TWIC holder riding in his/her cab. The owner/operator may grant this request at his/her discretion. The passenger most likely does not require frequent unescorted access and therefore does not need to

obtain a TWIC. However, the ultimate responsibility for meeting escort requirements rests on the owner/operator and he/she should verify that the driver can meet all of those responsibilities before allowing the driver to serve as an escort.

3.3 c.(2) (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.

1) The following situations would meet the requirements for monitoring. While they do not cover every situation, they should illustrate to owners/operators what could be acceptable as a monitoring protocol.

   EXAMPLE: An individual without a TWIC is sent on a task in a secure but non-restricted area which the supervisor, who has a TWIC, knows will take 10 minutes. If the individual without a TWIC does not check back in with the supervisor in 10 minutes, the supervisor will go to find the individual. The duration of the task should be short and the task should not take the individual into any restricted areas as side-by-side accompaniment would be required in those situations.

   EXAMPLE: The crew (TWIC holders) may monitor a work group or "persons in addition to crew" on a vessel underway when the work group is on duty by observing them while they are carrying out their assigned tasks and while the work group is off duty by ensuring that they do not enter any spaces where they are not authorized. The vessel owner/operator is encouraged to brief non-TWIC holders at the start of the voyage on the location of spaces where they are not authorized.

2) 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.** Owners or operators should ensure that adequate measures (e.g. security patrols) are in place to respond to unauthorized activities.
3) Other arrangements, including but not limited to security patrols or roving watches, automatic intrusion-detection devices, or surveillance equipment may be acceptable as long as they provide a reasonable assurance that an individual under escort is not engaging in activities other than those for which access was granted. In all cases, there must be an ability to communicate a breach of security in accordance with the existing approved security plan.

3.3 c.(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, appropriate physical accompaniment exists with one TWIC holder escorting no more than five non-TWIC holders. Owners/operators that choose a different physical accompaniment criteria will likely receive increased scrutiny from COTPs. Owners/operators are strongly encouraged to discuss deviations from this number with the COTP.

(4) Escorting ratios do not apply when non-TWIC holders are transported in an enclosed vehicle. In this case, one TWIC holder who is driving or riding in the vehicle can escort any number of passengers as long as they are only allowed to depart the vehicle in a location where other TWIC holders will be able to escort them or where they will not need to be escorted (e.g. a public access area or outside the facility). This applies in both secure areas that are restricted areas and secure areas that are not also restricted areas. Escorting requirements must be met once the non-TWIC holders depart the vehicle.

(5) Passengers may be considered escorted in the holding, waiting, or embarkation areas of cruise ship terminals, even though these are generally designated as restricted areas, since cruise ship terminals are already required to have additional security personnel in these areas who can meet the requirements for escorting in accordance with 33 CFR 105.290. If cruise ship terminal owners/operators use this option, the security personnel must have TWICs.

(6) During periods where portions of a facility are temporarily shut down for repairs and large groups of labor are brought in to perform the work (e.g. a turn-around at an oil refinery) escorting can be performed by isolating the area of work and controlling access through fencing or other means to ensure that workers remain only in the area of work. Workers need to be escorted from the facility entrance, through the secure area, to the work area and some means need to be in place to ensure that they do not leave the work area and gain unescorted access to the secure area of the facility. Means to ensure that workers do not gain unescorted access include patrols of the perimeter of the work area, observation through a CCTV system, or other equivalent measures. Once the work is complete and before resuming normal escorting procedures, a security sweep must be conducted to ensure that no unauthorized persons and/or dangerous substances and devices are present in the secure area. Approval for temporary escorting measures under this option must be obtained from the COTP prior to beginning work.

(7) Vessel crew changes, authorized shore leave, crew transportation to and from vessels via taxi or shuttle bus, and access to shoreside support should be facilitated to the maximum extent possible without compromising security or safety. Monitoring within secure areas could provide sufficient flexibility to support such important activities. In the case of restricted areas within the secure area, authorized TWIC holders, who are already working in the area, could provide the side-by-side accompaniment for the limited amount of time needed

before the transition back to the secure area takes place. Additional flexibility also exists to support these activities in some parts of the restricted area since the TWIC requirements will not apply to mariners while in the immediate vicinity of their vessel when performing routine ships business (in which mustering for transportation off the facility can be included). Regardless of which methods are used to comply with the TWIC requirements, facility owners and operators should work with COTPs to develop solutions which maintain security while facilitating the essential need for seafarers' access to shoreside support and authorized shore leave.

3.3 c.(8) In all cases, owners/operators must provide a sufficient quick response capability and respond immediately when an individual "under escort" enters an area where he/she has not been authorized to go or engages in activities other than those for which escorted access was granted. If this occurs, it is a breach of security. Sufficient quick response capability can be provided by, but is not limited to, security personnel with communications gear and transportation appropriate to the size of the facility, or watchstanders able to communicate with a roving watch.

(9) The regulations also require that new hires be accompanied by an individual with a TWIC in secure areas. Accompaniment for this purpose is explained in section 3.3 h. (1) (d) below and is not the same as the general escorting requirements.

ESCORT GUIDANCE	SECURE AREAS THAT ARE NOT ALSO RESTRICTED AREAS	PORTIONS OF SECURE AREAS THAT ARE ALSO RESTRICTED AREAS * *AS DEFINED IN FSP OR VSP
TWIC HOLDERS	UNESCORTED	UNESCORTED
LOST, STOLEN OR DAMAGED TWICS SEE 3.3 h (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 h (1) BELOW FOR FURTHER INFORMATION	ACCOMPANIED ACCESS FOR 30 CONSECUTIVE DAYS (WITH ADDITIONAL 30 DAYS AT COTP DISCRETION)	ACCOMPANIED ACCESS FOR 30 CONSECUTIVE DAYS (WITH ADDITIONAL 30 DAYS AT COTP DISCRETION – MONITORING
NON-TWIC SEE 3.3 C ABOVE FOR FURTHER INFORMATION	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TWIC TO 10 ESCORTED) OR MONITORING	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TWIC TO 5 ESCORTED)
U.S. MARINERS	UNESCORTED ACCESS DURING TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL AS LISTED IN 3.3 h (3) b)	UNESCORTED ACCESS DURING TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL AS LISTED IN 3.3 h (3) b)
FOREIGN MARINERS	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TWIC TO 10 ESCORTED) OR MONITORING (CAN WORK ADJACENT TO VESSEL W/O TWIC)	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TWIC TO 5 ESCORTED) (CAN WORK ADJACENT TO VESSEL W/O TWIC)

Table 2 – Escort guidance for secure areas that are not also restricted areas and secure areas that are also restricted areas

3.3 d. Employee Notification Requirement

(1) Facility and vessel owners/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/operators to determine which of their employees will need a TWIC and inform those employees in enough time for them to apply for a TWIC and comply with the requirements. Owners/operators are also encouraged, but not required, to provide this same information to personnel who are not facility or vessel employees, e.g. contractors, longshoremen, etc.

(2) Notification should assist employees 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.

3.3 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, five years from the last plan approval date. However, for passenger vessels and ferries, the visual representation of passenger and employee access areas (see section 3.5) must be incorporated in the VSP at the next VSP submittal, either renewal or amendment. **While facility and vessel owners/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).** Owners/operators are not required to add TWIC Program provisions to security plans by this rule because a follow-on rulemaking is planned which will include TWIC reader requirements and a provision requiring an update to security plans. Instead of requiring two amendments in a short time frame, only one amendment will be required after the second rule. However, facilities who desire the benefit of reducing their secure area must submit an amendment to their FSP now.

(2) Facility owners/operators desiring to redefine their secure area 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 plan approval date. The security plan must still cover the entire facility as originally submitted. The intent of providing this optional provision is to redefine 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 details on this option, see section 3.4.

3.3 e.(3) Facility owners/operators participating in one of the approved Alternative Security Programs (ASP) may also request to redefine their secure area if the sponsoring organization of the ASP has amended it to allow for redefinition of secure areas. For details on this option, see section 3.4.

3.3 f. Incorporation of the TWIC into Existing Physical Access Control Systems

(1) Vessels and facilities 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. Vessel or facility-specific 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/operators need to ensure that their own access control systems are updated to show whether the employee has a TWIC, even when an employee presents only the vessel or facility-specific card, and must have a way to cancel or deactivate the vessel or facility-specific card when the TWIC has expired.

> **EXAMPLE:** A facility employee who possesses a valid TWIC is registered into the facility's access control database and is issued a facility access card after the TWIC is verified visually as described in 3.3 a. (7). To gain entry into a secure area, the employee inserts or scans his/her facility access card at a card reader, which verifies the access card as a valid card for the facility. The TWIC does not need to be used as a visual identity badge at each entry once the facility-specific card is issued. The card reader then verifies the individual by matching the facility access card to the individual's record in the facility database and allows access to secure areas as dictated by the permissions established by the owner/operator in the access control system. By virtue of the fact that the employee would not be issued a vessel or facility-specific card without first having a TWIC, the requirement to possess a TWIC for unescorted access to secure areas is met.

As the TWIC is not used as a visual identification badge on a daily basis, random visual checks for TWICs, as described in 3.3 a., shall be implemented to ensure that employees continue to keep their TWIC on their person or in close proximity to their work station (within 10 minutes). The facility may also ensure that the employee's TWIC has not been revoked by comparing its employee records to the TSA list of invalidated TWICs, but this is not required. The only requirement is that once a TWIC expires, according to the date printed on the TWIC, the vessel or facility-specific card must deny unescorted access to secure areas. **In no situation should an employee be issued a vessel or facility-specific card which allows unescorted access to a secure area without first ensuring that the individual possesses a TWIC.**

3.3 f. (2) Although not required, owners/operators may implement biometric card readers and systems in order to confirm identity of 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 geometry). 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/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 because they are using the vessel or facility-specific card, they must always have the TWIC on their person or readily available while in a secure area in accordance with 33 CFR 101.515 (d). The TWIC will be required for unannounced Coast Guard spot checks and annual inspections, as well as internal vessel or facility security checks, when implemented. Owners/operators may require personnel to visibly display the TWIC at all times while on a facility or aboard a vessel if company policy dictates. However, if owners/operators determine that having their personnel physically maintain the TWIC on their person is impractical, the TWIC may be secured in a convenient location where it can be retrieved and presented in no more than 10 minutes for inspection or examination. Having a separate access control system will not exempt employees from having TWICs on their person or readily available as discussed above. Any individual found unescorted without a TWIC in a secure area will be considered a breach of security to be handled according to the procedures documented in currently approved security plans. Owners/operators should consider implementing random checks of TWICs at access points to ensure individuals always have the TWIC on their person or readily available as discussed above. A description of how the TWIC is incorporated into existing physical access control systems should be included in the security plan in the next regularly scheduled submission.

3.3 g. Knowledge Requirements for Personnel

(1) Company (CSO), Vessel (VSO), and Facility Security Officers (FSO):
In accordance with 33 CFR 104.210, 104.215, 105.205, and 106.206, 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
- Recognition of a valid TWIC in accordance with section 3.3a of this NVIC
- Escorting requirements
- Integration of the TWIC Program into existing access control systems

- Resolution of violations (forged or tampered TWICs, security breaches) [See Enclosure (4)]
- 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

3.3 g. (2) Company, vessel, and facility personnel with security duties:
In accordance with 33 CFR 104.220, 105.210, and 106.215, company, vessel, and facility personnel with security duties 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

(3) All other company, vessel or facility personnel:
In accordance with 33 CFR 104.225, 105.215, and 106.220, all other company, vessel, or facility personnel will be knowledgeable in, and shall be able to demonstrate familiarity with the relevant TWIC Program requirements as they relate to the vessel or facility, specifically:

- How TWIC applies to the vessel or facility
- Recognition of a valid TWIC
- Location of secure, restricted, and passenger/employee access areas, as applicable
- Procedures for reporting lost, stolen, or damaged cards
- Escorting procedures

3.3 h. Special Provisions for Access Control

(1) New hires
This provision is intended to limit the risk presented by certain individuals who have not undergone a full security threat assessment and have 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 a name-based security check has been completed. This provision is granted at the owner/operator discretion and only applies to direct employees. Therefore, owners/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 applied for but not yet received a TWIC (hereafter referred to as a new hire), the owner/operator may grant the individual accompanied access to secure areas of the vessel or facility. Accompanied access is explained in paragraph (d) below. This accompanied access may be granted for a period of up to 30 consecutive calendar days from the date of TWIC enrollment, after notification through Homeport that the individual has passed the name-based check. Accompanied access may be extended for an additional 30 days by the cognizant COTP (the COTP of the zone where the applicant enrolled) if TSA has not yet issued the new hire's TWIC.

3.3 h.(1) (a) The following steps must be completed prior to granting accompanied access to new hires:

1) 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/operator has the individual sign a statement affirming this. There is no required format for this statement. A form can be developed by the owner/operator as needed. This form must be retained until the new hire receives his/her TWIC.
2) The owner/operator or CSO/VSO/FSO shall be able to articulate an adverse impact to vessel or facility operations if each new hire is not granted accompanied access before being issued their TWIC. This impact may be requested by Coast Guard personnel during inspections and spot checks.
3) The individual can present another identification credential that meets the requirements of 33 CFR 101.515.
4) 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.
5) The owner/operator or CSO/VSO/FSO 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. Owner/operators, CSO's , VSO's, and FSO's will need to register on Homeport in order to be able to enter new hire information if they do not already have a login and password. For the new hire provision only, the owner/operator, CSO, VSO, or FSO registered in Homeport for that vessel

or facility may use Homeport to view the status of the name-based security check of their newly hired employees. A new page is being developed in Homeport for submission of new hire information and will be available before the first expected compliance date. Detailed instructions on how to enter new hire data will be posted on Homeport once the functionality is ready. In order for this status to be posted for the owner/operator, CSO, VSO, or FSO 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 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 name-based check will not be returned.**

3.3 h.(1) (b) This section may not be used to grant temporary accompanied access to an individual being hired as a CSO, VSO, or FSO 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. Security as a primary duty means individuals whose fundamental responsibilities focus on security of the vessel or facility. These positions include security guards, baggage screeners, and persons making access control decisions. It does not include individuals who perform security duties as an occasional task or as a collateral duty.

(c) The owner/operator, CSO, VSO, or FSO must wait for a notification that the new hire has passed the name-based check in Homeport before accompanied access can be given to the individual. The owner/operator or CSO/VSO/FSO may log into Homeport at any time after submitting the new hire's information to check the status of the name-based check. However, the Homeport system is designed to automatically send an email to the owner/operator, CSO, VSO, or FSO, which will prompt them to log in to Homeport when the new hire has passed the name-based check (or if the information needs to be resubmitted). Due to privacy and security concerns, Homeport will not email information on the status of a new hire directly to the owner/operator or CSO/VSO/FSO. Instead, users must log in to Homeport to access this information. The 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 numbers 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.

3.3 h.(1) (d) 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 total vessel or facility work unit TWIC-holding employees may be allowed to have access under this provision at any 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 currently approved security plan must be followed, with the addition of the TWIC requirements. If certain measures are not able to be followed for an extended period of time due to maintenance or repairs (e.g. 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) Specific guidance for vessels or facilities is noted below:
   i. Vessels
      - This provision is only available to vessels with a total required crew compliment not exceeding 10 persons.
      - For a vessel with a Certificate of Inspection (COI), the total required crew includes all personnel in the required manning section. The total crew does not include the following categories listed on the COI: persons in addition to crew, passengers, and other crewmembers.
      - For vessels without a COI, the total required crew includes all personnel performing navigation, safety, and security functions. This includes, but is not limited to, all licensed and documented mariners.
      - The total number of vessel employees for computing the maximum number of new hires allowed includes all personnel assigned to the vessel who are required to obtain a TWIC. This number **may be greater** than the crew listed on the COI or manning document if personnel other than the crew need unescorted access to secure areas or are mariners. On a vessel that does not maintain the same crew onboard for 24 hours a day, the number of new hires is determined by the number of employees requiring TWICs onboard for that shift.

        EXAMPLE: A vessel has seven total crew on its COI and has 21 total employees requiring TWICs (14 “other persons in crew”). This vessel is eligible to use the new hire provision because it has less that 10 total required crew on its COI. The total number of new hires allowed would be 25% x 21 = 5.25.

This is then rounded up to six. This vessel is allowed no more than six new hires at any given time.

- The individual may be considered accompanied in their assigned work area and living areas (e.g. berthing areas, mess areas, recreation areas, heads) as long as all criteria in d)1), d)2), and d)3)i) are met. If a new hire is working in a restricted area, they must be monitored in accordance with 3.3c.(2)(b).

3.3 h.(1) (d) 3)ii. 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 total number of TWIC holders in each work-unit may be new hires. See guidance in d)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 all criteria in d)1), d)2), and d)3)ii) are met. 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.

Who can use the New Hire Provision?	
Individual must meet <u>all</u> of the following criteria:	• Is a newly hired direct employee • Has completed the application process for a TWIC but has not yet received TWIC • Has not applied for a waiver or is not in appeal process • Needs immediate access to secure areas for performance of duties • Is not a CSO/VSO/FSO or does not perform security as a primary duty • Can present another form of identification for access • There are no other circumstances that would cause reasonable suspicion
Vessel must meet <u>all</u> of the following criteria:	• Total crew does not exceed 10 individuals (as required by the COI or other manning document) • The number of new hires allowed at any time must be no more than 25% (rounded up to the nearest whole number) of the number of employees requiring TWICs onboard
Facility must meet <u>all</u> of the following criteria:	• Work unit does not exceed 25 individuals • The number of new hires allowed at any time must be no more than 25% (rounded up to the nearest whole number) of the number of employees requiring TWICs within the work unit

Table 3 – Criteria for individuals, vessels, and facilities to use the new hire provision

TWIC New Hire Provision Process

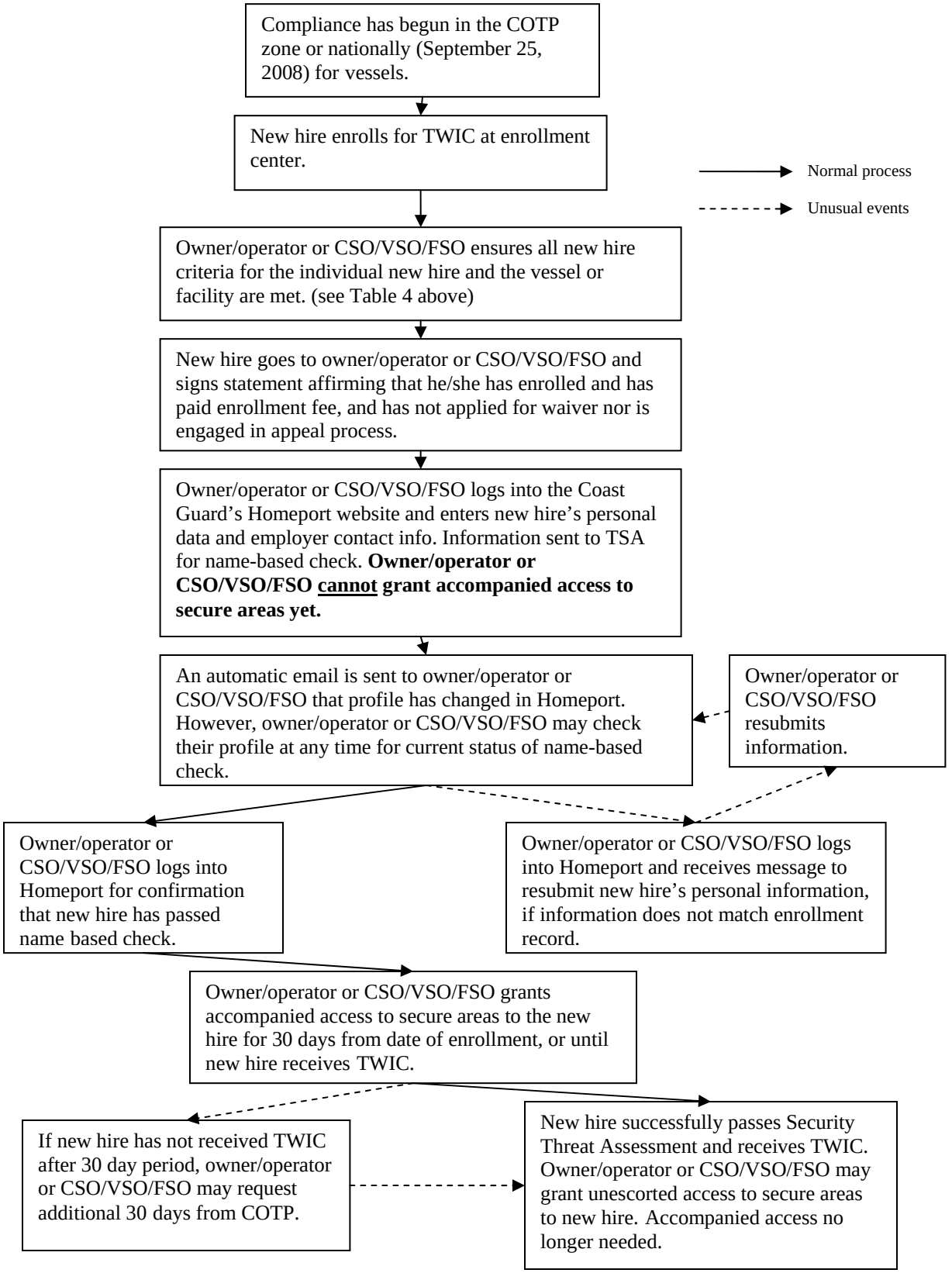


Figure 5 – Chart describing the steps before a new hire can be given accompanied access

3.3 h.(2) Lost, stolen, or damaged TWICs

If an individual's TWIC is lost, stolen, or damaged, he/she must report it immediately to TSA (through the TSA TWIC help desk at 1-866-DHS-TWIC) as required in 49 CFR 1572.21. TSA will revoke the lost, stolen, or damaged TWIC and begin the process of producing a new card, which must be picked up at an enrollment center designated by the individual. During that period after the TWIC has been reported as lost, stolen, or damaged and while a new TWIC is being produced, the individual may be granted unescorted access to secure areas of the facility or vessel for seven consecutive calendar days under the following circumstances:

(a) The individual can present another identification credential that meets the requirements of 33 CFR 101.515.

(b) The owner/operator, CSO, VSO or FSO verifies that the individual had a valid TWIC and has previously been granted unescorted access to secure areas of the vessel or facility (recommended within the past 90 days). This can be done by checking employee lists, records of access, or knowledge of security staff.

(c) The individual has reported the TWIC as lost, stolen, or damaged to TSA as required in 49 CFR 1572.21. Currently, no procedures are available for the CSO, VSO, or FSO to check that the card has been reported as lost, stolen, or damaged. However, given the seven day limitation, it is in the TWIC-holder's best interest to ensure that his/her TWIC 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 seven days expire.

(d) There are no other suspicious circumstances associated with the individual's claim of loss, theft, or damage. 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.

(e) For vessels continuously underway for greater than seven days, the above procedures can be initiated as soon as the individual returns to a port in the U.S., or a U.S. territory where TWIC enrollment centers are operational, and the seven day allowance will begin at that time.

Because the individual is granted unescorted access under this provision for no longer than seven consecutive calendar days, he/she should pick up his/her card as soon as he/she is informed by TSA that it is available.

(3) Access control during the enrollment phase-in period

Over the course of the 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, individuals in mobile populations may be traveling from an area where enrollment has not begun to an area where compliance has started.

(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. Therefore, 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.

3.3 h.(3)(b) Merchant mariner access

Because mariners are a large, inherently mobile population, they will not be required to possess a TWIC for unescorted access to vessels or facilities during the enrollment period. This matches the national vessel compliance date of September 25, 2008. However, during the enrollment period, in order for a mariner to be eligible for unescorted access through 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 valid photo identification
- CG COR and a valid photo identification

Mariners are eligible to escort non-TWIC holders under this provision, provided the owner/operator allows mariners to serve as escorts. The identifications listed above are the only forms of identification that will be accepted in lieu of a TWIC because they incorporate a comparable threat assessment conducted by the Federal government. This provision was not intended for vessel personnel who do not have licenses or documents, such as deckhands and crew on inland towing vessels. These individuals should not apply for one of the identifications listed above in order to qualify for this provision. If unescorted access is needed and the individual does not already possess one of the forms of identification listed above, he/she should apply for a TWIC. 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 September 25, 2008, mariners will need a TWIC for unescorted access to secure areas of vessels and facilities.**

3.3 i. Area Maritime Security (AMS) Committee Members

AMS Committee members who require access to SSE and who do not hold a TWIC in the course of their work, are not a credentialed Federal, state, or local official, or do not have a comparable threat assessment as determined by TSA, are required to undergo a name-based 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. Federal Maritime Security Coordinators (FMSCs) will enter the names of the AMS Committee members who do not possess a TWIC into Homeport by **September 1, 2008**. Guidance to FMSCs for submitting AMS member information will be provided via message traffic.

3.3 j. Waivers, Exemptions, and Equivalencies of TWIC Requirements

(1) 46 U.S.C § 70105 is clear on the applicability of TWIC. Therefore, the Coast Guard anticipates that the TWIC requirements will be necessary for applicable vessels and facilities. As a result, the Coast Guard 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/operators may request a waiver from any provision in the regulation. Vessel and facility owners/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 (c) through (e).

(2) The only parties who are required to submit amendments are those facilities with a significant non-maritime transportation component that want to redefine their secure area. All other owners/operators are not required to submit TWIC amendments to approved security plans. Amendments to redefine the secure area for other 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, however all other MTSA requirements remain unchanged. 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 the United States Code for details on these waivers. However, when these vessels are not operating under these waivers (e.g. 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, 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/operators from TWIC requirements at this time.

(5) Current regulations in 33 CFR 101.130, 104.135, 105.135, and 106.130 allow owners/operators to propose an equivalent 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. Elements of proposed equivalent credentialing programs will be measured against TWIC Program elements including but 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 (ASPs) remain valid and do not have to be resubmitted, except for ASPs which have facility participants who want to redefine their secure area. All ASP sponsoring organizations may wish to resubmit their ASPs to incorporate TWIC Programs in accordance with 33 CFR 101.120, though this is not required. If ASP sponsors desire to allow member

facilities with significant non-maritime transportation portions of their facilities to redefine secure areas, then the ASP must be amended. See section 3.4 c. for more information.

3.4 Facility-specific Guidance

3.4 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 frequently access secure areas of maritime transportation vessels and facilities. Although the TWIC rule does not alter the MTSA-regulated geographic area of a facility, it does permit those facilities with a significant non-maritime transportation portion to submit for approval an amendment to their FSP to redefine their secure area to cover only the maritime transportation portion of the facility. **The rest of the FSP must still cover the facility as originally submitted.** The intent of this provision is to limit TWIC applicability to the maritime transportation portion, not to reduce the area over which the FSP applies.

(2) Facilities with a significant non-maritime transportation portion may apply to the COTP to redefine their secure areas for purposes of TWIC. COTPs will assess the feasibility of the request, taking into account the risk of a transportation security incident from the maritime transportation related portion. Facilities that may be considered to have a significant non-maritime transportation portion include, but are not limited to, refineries, chemical plants, factories, mills, power plants, smelting operations, and recreational boat marinas. The Coast Guard will generally not consider the following for exclusion from a secure area: commercial docks, container yards, passenger terminals, and storage areas or tank farms that are specifically used to stage cargo for loading to a vessel or to receive cargo at its first point of rest upon discharge from a vessel.

(3) Some restricted areas may be authorized to lie outside the secure area if owners/operators can demonstrate that they do not directly support or interface with the maritime transportation related portions of the facility. The Coast Guard will generally consider that the following restricted areas have a maritime transportation nexus and should always be included in the secure area:

(a) Shore areas immediately adjacent to each vessel moored at the facility
(b) Areas designated for loading, unloading or storage of cargo and stores*
(c) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes*.

*However, in some cases, tank farms or cargo storage areas directly support both maritime transportation and industrial processes (e.g. a coal pile supplied by vessel and consumed in a power plant or a tank farm storing product refined onsite intended for shipment by a vessel). In determining whether these directly support or interface with the maritime transportation portion of the facility, owners/operators should consider the following: risk of a TSI, proximity to vessels and the waterfront, and hazards of cargo. The Coast Guard expects that cargo storage areas near vessels or the waterfront will be included in the secure area, regardless of whether or not they also serve an industrial purpose.

3.4 a. (4) The redefined secure area must have sufficient access control measures such as fencing, gates, monitoring, etc., in order to deter and restrict unauthorized persons from gaining access to the secure area. In accordance with 33 CFR 105.310 (c), the facility owner/operator must review and validate the Facility Security Assessment (FSA), and update the FSA report to reflect the redefined secure area. Plans for how access control will be conducted for the redefined secure area must be included in the amendment to the FSP. The submission to the COTP must include the FSP amendment with the new FSA report and a justification detailing the reasons the particular portions of the facility have been included in the redefined secure area. All amendments must be submitted to the COTP no later than 60 days after the publishing date of this NVIC (September 4, 2007). Facilities that have an approved letter of intent must file an amendment with the COTP by this deadline. 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.

3.4 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 (c) with additional requirements as detailed above.

3.4 c. Facilities participating in an ASP

Facility owners/operators participating in one of the approved ASPs may also request to redefine their secure area if the ASP has an approved amendment to allow for this.

1) First, the sponsoring organization must submit an amendment to the ASP for review and approval by Commandant. This amendment shall state that member facilities must submit redefined secure area proposals to local COTPs for review and approval. ASPs shall include the format for member facility submissions and only the redefined secure area will be open for review and approval by the COTP. ASP amendments must be submitted to Commandant (CG-3PC) as early as possible; we recommend no later than 60 days after the publication of this NVIC. This early submission is critical to enable facilities participating in the ASP to submit their redefinition requests to the local COTP in time for review and approval prior to the compliance date for that particular COTP zone.
2) Once the ASP amendment is approved by Commandant (CG-3PC), individual facilities shall request redefinition of their secure area from the local COTP for review and approval. Individual facilities shall include a justification detailing the reasons the particular portions of the facility have been included in the redefined secure area and include the same restricted areas as listed above in 3.4(1). As redefinition of the secure area is optional and an on-site evaluation of the request may be required, facility owners/operators desiring to redefine their secure area must submit their proposals directly to the COTP for local review and approval, which is a new process for most ASP participants. Requests to redefine secure areas should be submitted to the local COTP in time to facilitate review and approval prior to the compliance date for that particular COTP zone.

3.5 Vessel-specific Guidance

3.5 a. 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 maritime transportation related. Therefore, the entire vessel is designated a secure area, with the exceptions of the passenger and employee access areas as discussed below.

3.5 b. Designation of 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 dining and entertainment, this rule establishes two areas applicable in passenger vessels and ferries where TWICs are not required. These areas 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 vessel's secure area. The rest of the vessel remains a secure area where TWICs are required 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/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 33 CFR 104.120(c). Vessels operating under an ASP must also maintain this visual representation onboard if they designate these areas. This visual representation does not need to be approved by the Coast Guard until the next VSP submission, but must be available during Coast Guard inspections. VSPs must be updated to include the visual representation with the next submission, either amendment or renewal.

(1) Passenger access areas are 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** (see 33 CFR 104.107).

3.5 c. Process for Vessel Personnel to Obtain TWICs and Credentials

Until the Merchant Mariner Credential rule is finalized, mariners will hold separate MMDs, Licenses, CORs, or STCW Endorsements, as needed, and will also need to hold a TWIC after September 25, 2008. The process for obtaining these documents is detailed below:

1) The process for an individual who only needs unescorted access to secure areas of a vessel and does not need a Coast Guard-issued license, MMD, COR, or STCW endorsement is the same as any other TWIC applicant and is described in Enclosure (2).

3.5 c.2) The process for an individual who needs to apply for, or to renew an existing license, MMD, COR, or STCW Endorsement, and to obtain a TWIC is below[3]:

(a) Mariner may pre-enroll to obtain a TWIC by visiting the TSA website at www.tsa.gov/twic, and make an appointment to complete enrollment at the enrollment center of their choosing.

(b) Mariner visits one of at least 130 TWIC enrollment sites to provide biographic information and a complete set of fingerprints, sit for a digital photograph, and pay the enrollment fee.

(c) Mariner then contacts one of seventeen Regional Exam Centers to renew/apply for an MMD, license, COR, STCW endorsement (as applicable). After September 25, 2008, the REC will not issue mariner document until TWIC has been issued, but applications can proceed concurrently.

(d) TSA will conduct a TWIC security threat assessment (if mariner does not yet possess an MMD or license).

(e) Mariner is notified by email or phone to pick-up their TWIC. Mariner chooses a PIN and the card is activated. TWIC is valid for a period of 5 years unless the applicant relied upon the security threat assessment done for their MMD/License, in which case the date of expiration will be the same as the MMD/License for which the security threat assessment was performed..

(f) Mariner completes the process with the REC and picks up their MMD, license, COR, or STCW endorsement. After September 25, 2008, the mariner must show his/her TWIC before the MMD/license/COR/STCW will be issued.

[3] If the MMC SNPRM is finalized, the steps to apply for or renew an MMC will change. Instead of both the REC and TSA collecting biographic and biometric information, only TSA will collect this information and will share it with the National Maritime Center (NMC) along with the results of the security threat assessment. Mariners will then apply for or renew their MMC via mail, unless an examination is required. The process for the TWIC application will remain the same.

Table of Contents

This page intentionally left blank

Enforcement Guidance

4.1 Enforcement Strategy

As with other maritime security initiatives, the Coast Guard will work cooperatively with facility and vessel owners/operators to implement and maintain compliance with the TWIC regulations. As this new program is rolled out, continued COTP collaboration with affected stakeholders will assist with these first steps toward increasing security throughout the maritime transportation system. For facilities and vessels in substantial compliance that are making a good faith effort to comply with the TWIC regulations, on-the-spot corrections could suffice to satisfy the Coast Guard, especially during the initial implementation and enforcement phases. For those vessels and facilities that are not in substantial compliance, progressive enforcement tools may be used such as a Letter of Warning, Notice of Violation (NOV) or other civil penalties. For egregious vessel and facility noncompliance, operational restrictions, including suspension of operations is an option. However, the latter should be used only after other attempts to gain compliance have been unsuccessful or such noncompliance creates an imminent security threat. More detailed enforcement guidance will be published before the first compliance date as a Coast Guard Commandant Instruction. This internal instruction will provide information for the COTP on the Spot Check Program and enforcement options available to gain compliance.

4.2 Enforcement Implementation

The Coast Guard intends on integrating TWIC Program compliance activities into our current vessel and facility inspection examination policies and does not anticipate adding inspections solely to verify compliance with TWIC requirements. The new requirements will be verified by Coast Guard personnel during annual compliance exams and periodic spot checks of each vessel and facility. During these activities, 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 not been revoked by TSA
- contain a biometric template that matches the fingerprint of the person carrying the TWIC.

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**.

4.3 Invalid/Fraudulent Cards

4.3 a. Owner/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/operator should, at a minimum:
    - Deny the individual unescorted access to secure areas of the facility or vessel. The owner/operator may, of course, grant escorted access. However, since tampering with or creating a fraudulent TWIC may be a violation of Federal law, great care should be exercised with respect to these individuals.
    - Check the person's identity by asking for one of the alternate forms of identification described in 33 CFR 101.515. 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, including the information on the TWIC. Make a photocopy of the TWIC if possible.

- Call the COTP, in conjunction with any notifications in the currently approved VSP or FSP, and 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 the TWIC is fraudulent. Follow any instructions that the duty officer provides.
- If directed by the Coast Guard, ask the individual to remain at the access control point until the Coast Guard or other law enforcement agency arrives. **The owner/operator is not required to make any attempt to restrain the individual or inform him/her that he/she may not leave.**
- The ability of the owner/operator to take a TWIC is dependent on state law. The Coast Guard cannot authorize the owner/operator to exercise law enforcement authority. Owners/operators should contact their own lawyers to discuss recommended actions for their specific state and vessel or facility.
- In the case of the expiration of particular types of non-immigrant visas [4], employers are required by regulation to retrieve the TWIC and return it to TSA.

4.3 a.2) Suspicious activity

As currently required by 33 CFR 101.305 (a), suspicious activity must be reported in accordance with the currently approved VSP or FSP. Suspicious activities related to TWIC include, but are not limited to:

- Multiple TWICs suspected to be fraudulent presented by different individuals for access in a short period of time (five to seven 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 him/her)
- Many different appearances of TWICs which are suspected to be fraudulent – a 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.

4.3 b. Possible Coast Guard Actions

1) The Coast Guard will advise the owner/operator of the vessel or facility whether an inspector will arrive to investigate the TWIC. The Coast Guard may respond to the vessel or facility to attempt to verify the TWIC using handheld readers.
   - 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 10 attempts, the Coast Guard may take custody of the suspect TWIC and will advise the vessel or facility owner/operator of any additional actions the vessel or facility should take.

[4] H-1B Special Occupations, H-1B1 Free Trade Agreement, E-1 Treaty Trader, E-3 Australian in Specialty Occupation, L-1 Intracompany Executive Transfer, O-1 Extraordinary Ability, or TN North American Free Trade Agreement

- Failure of an individual to match the biometric template to his/her fingerprint does not conclusively prove that he/she is not the rightful owner of the TWIC. Electronic and environmental reasons may interfere with the matching and will be addressed in the Coast Guard enforcement Commandant Instruction.

4.3 b. 2) If the Coast Guard will not dispatch personnel to a particular situation, the vessel or facility owner/operator will be so advised.

This page intentionally left blank

Implementation Schedule

This Enclosure will be updated once the schedule is available and will be a link to the online schedule to allow for easy access to the most current version of the schedule.