TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL PROGRAM: SMALL ENTITY GUIDE FOR OWNERS AND OPERATORS

PUBLICATION DATE: SEPTEMBER 14, 2007

This Page Intentionally Left Blank

TABLE OF CONTENTS

LIST OF TABLES

Foreword

WHY TSA AND USCG WROTE THIS GUIDE

The United States Coast Guard (USCG) and the Transportation Security Administration (TSA) wrote this guide to inform you about how the Transportation Worker Identification Credential (TWIC) rules apply to you and to help you comply with the program requirements. This guide tells you about your responsibilities and obligations under the TWIC program. You will find information you need to know to comply with the rules.

USERS' RIGHT TO REPRODUCE THIS GUIDE

This guide is in the public domain. That means you may copy this guide without asking anyone. Please reference where you got the information. Cite this guide as: Transportation Worker Identification Credential Program: Small Entity Guide for Owners and Operators.

WHERE TO GET THIS GUIDE ELECTRONICALLY

You can find an electronic copy of this guide at three different websites. You can save an electronic copy for your files or you can print this guide. The three websites are:

- The Docket Management Facility's website at http://dms.dot.gov in the TSA's and the USCG's dockets numbered TSA-2006-24191 and Coast Guard-2006-24196.
- The USCG's Homeport website under the Maritime Security/TWIC heading at http://homeport.uscg.mil.
- The TSA's website at http://www.tsa.gov/twic.

Terms Used in this Guide

ASP	*Area Security Plan.*
CFR	Code of Federal Regulations.
COTP	Captain of the Port.
CSO	Company Security Officer.
DHS	Department of Homeland Security.
Facility	A facility subject to 33 CFR part 105.
FSO	Facility Security Officer.
FSP	A USCG approved Facility Security Plan.
ID	A means of identification, such as a document containing official information. The TWIC is a form of ID.
Maritime Facility	A facility subject to 33 CFR part 105 or an OCS facility subject to 33 CFR part 106.
MARSEC	Maritime Security (Level).
MODU	Mobile Offshore Drilling Unit.
MTSA	Maritime Transportation Security Act of 2002.
NTSB	National Transportation Safety Board.
NVIC	Navigation and Vessel Inspection Circular.
OCS Facility	An outer continental shelf facility subject to 33 CFR part 106.
OSV	Offshore Supply Vessel.

Operator	Operator of a vessel or maritime facility.
Owner	Owner of a vessel or maritime facility.
PIN	Personal Identification Number.
SAFE Port Act	Security and Accountability for Every Port Act of 2006.
Secretary	Secretary of DHS.
STA	Security Threat Assessment.
TSA	Transportation Security Administration.
TSI	Transportation Security Incident.
TWIC	Transportation Worker Identification Credential.
TWIC Program	The procedures and systems to check and validate transportation worker access control measures.
USCG	United States Coast Guard.
Vessel	A vessel subject to 33 CFR part 104.
VSO	Vessel Security Officer.
VSP	A USCG approved Vessel Security Plan.
We, us	USCG and TSA.
Worker	A transportation worker subject to the TWIC program.
You, your	*The reader (usually the owner or operator of a vessel or maritime facility).*

About This Guide

This guide is for you if you are the owner or operator of a vessel or maritime facility under the TWIC program. This guide also has general information about the TWIC rules.

(There is another guide for TWIC applicants and holders. It provides information on who must get a TWIC, who is eligible to get a TWIC, TWIC holder responsibilities, and other useful information. The title of that guide is, *Transportation Worker Identification Credential Program: Small Entity Guide for Applicants*)

HOW TO USE THIS GUIDE TO LEARN ABOUT THE TWIC PROGRAM

Our TWIC rules are in the Code of Federal Regulations (CFR) in titles 33, 46, and 49. This *Small Entity Guide for Owners and Operators* takes the important information in the rules that may affect you and puts it in one place. We hope it helps you understand the requirements of the TWIC program. You can use the section above, titled *Terms Used in This Guide*, as a reference to understand words and abbreviations we use. Use the headings in the table of contents to find where to look in this guide for information you want to know. Read the whole guide to understand the TWIC rules better.

Use the tables and text boxes to find things we want to highlight about the rules. Some tables explain important rule language to make it easier to understand. Use the websites and call centers tables to find out where you can get help or find more information.

THIS GUIDE DOES NOT REPLACE THE RULES

This *Small Entity Guide for Owners and Operators* is not a substitute for the rules nor is it itself a rule. It is not intended to nor does it impose legally binding requirements. You must comply with the rules, and we hope this guide will help you understand the requirements in the statutes and regulations that apply to you. You may use an alternate approach to those found here if the approach satisfies the applicable regulations. Check our websites for changes in the TWIC program or in how we will enforce the rules.

Responsible Agencies

TSA and USCG published the TWIC rules together. We are both responsible for letting you know about the program, and we have set up sources to help you comply. You can find those sources in the part of this guide titled, *Where to go for Information and Assistance*.

WHAT TSA DOES

TSA enrolls TWIC applicants, performs the security threat assessments, issues and revokes TWICs, and renews TWICs. We have the following responsibilities.

- Set up enrollment centers (staff and facilities).
- Publish notices in the *Federal Register* telling applicants where and when to enroll.
- Enroll applicants and issue TWICs.
- Conduct the Security Threat Assessment (STA) processes.
- Handle waivers and appeals.
- Use appropriate data to check on TWIC holders during the life of their TWICs.
- Work with local authorities, owners and operators, and USCG in cases of imminent security threats.

WHAT USCG DOES

USCG enforces the TWIC program as an access control measure. We incorporate compliance with the TWIC program into current inspection policies. We have the following responsibilities.

- Give guidance and assist industry to implement the TWIC program.
- Make annual compliance inspections.
- Spot-check vessels and maritime facilities to ensure they have working TWIC programs, check fingerprints, and match biometrics on TWICs.
- Review Vessel Security Plans (VSPs) and Facility Security Plans (FSPs). In the future, we will include review to make sure TWIC is part of an overall security program.
- Work with local groups to make sure people know when to comply, where to enroll, and how to get any other useful information.
- Work with vessel and maritime facility inspection teams and industry staff to make permanent security improvements.
- In some cases, respond to reports of invalid or false TWICs.

Where to Go for Information and Assistance

If you are an owner or operator, you must tell your employees certain things about the TWIC program. Also, there are USCG and TSA resources like websites and call centers to help people apply for a TWIC. They will help answer your questions related to eligibility, enrollment, or compliance. USCG and TSA staff operate some of these resources. Government-hired contractors operate others.

Things your must tell your employees

- Where there are secure areas.
- If they need unescorted access.
- About any secure, public, employee, or passenger access areas.
- When we will start to enforce the TWIC rules in your area.
- When and where they can apply for a TWIC.

WHAT TO TELL YOUR EMPLOYEES ABOUT THE TWIC APPLICATION PROCESS

To help your employees apply for a TWIC, you must tell them who must get and maintain a TWIC, how to apply for it, and the deadline for applying. We want you to do this because you authorize unescorted access. You must provide your employees with enough notice for them to apply and get a TWIC when they need it.

You might notify your employees in some of the following ways.

- Signs posted in common areas.
- Company newsletters.
- Announcements by company officials.
- Company website.
- Inserts in wage and salary statements or other payroll documents.

We hope you will tell other workers about the program even if these workers are not employees. For example, if there are contractors or truckers who must have unescorted access to a secure area, encourage them to check common areas, newsletters, and your website for news about the TWIC program.

IF YOU ARE NOT THE WORKER'S EMPLOYER

If you hire workers who are not your employees, tell their employers which jobs require the worker to get a TWIC.

FOR A WORKER WHO IS SELF-EMPLOYED

If a worker is self-employed, but regularly works at your maritime facility or vessel, it is in everyone's best interest for you to tell that person if he or she needs a TWIC to do the job. Make sure your Facility Security Officer (FSO), Company Security Officer (CSO), or Vessel Security Officer (VSO) knows which workers need a TWIC.

THE TWIC RULES

The first time we publish any rule, that rule must go in the Federal government's "daily newspaper" for agencies – the *Federal Register*.

At the beginning of the rule – in a section called the preamble – we explain to readers what we think about the rule. We also explain how we addressed comments on the proposed rule. The preamble is a good place to find information about our intent and about the rules.

We published the TWIC program rules in the *Federal Register* on January 25, 2007 (72 FR 3491). The rules are titled *Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License*. They changed the following CFR parts.

- 33 CFR parts 101, 103, 104, 105, 106, and 125.
- 46 CFR parts 10, 12, and 15.
- 49 CFR parts 1515, 1540, 1570, and 1572.

You can get the *Federal Register* rules and preamble, and any related correction documents, from the following sources.

- The Coast Guard's Homeport website under the Maritime Security/TWIC heading at http://homeport.uscg.mil.
- Government Printing Office website at http://www.gpoaccess.gov/fr/index.html.
- The *Federal Register* website at http://www.archives.gov/federal-register.

Many libraries around the country agree to keep the *Federal Register*, and you can find the *Federal Register* in any such *depository library*.

You also may find the rules and related documents in dockets TSA-2006-24191 and Coast Guard-2006-24196. Except for Federal holidays, you may inspect and copy materials in the docket in person between 7 a.m. and 5 p.m., Monday through Friday, at the following address.

Docket Management Facility
U. S. Department of Transportation
1200 New Jersey Ave., S.W.
Washington, D.C. 20590

You may see the docket on the internet, 24 hours a day, 365 days a year, at http://dms.dot.gov.

TWIC ENROLLMENT CENTERS

To get a TWIC, a worker must enroll in the program in person at a TSA enrollment center. We will phase-in the TWIC program, which means we will start in one port and then open in other ports as time goes on. TSA contractors will set up and operate enrollment centers and issue TWICs under our rules. (We talk more about phase-in later in this part.) We will provide the biggest enrollment capacity until September 25, 2008, when everyone will need a TWIC. Our goal is to have at least one enrollment center in each of about 130 ports across the country.

Some of these centers may not be permanent. Some will reduce staff after the phase-in period. Although a worker may apply at any enrollment center, encourage your employees and other workers to apply for a TWIC at the peak enrollment time in your local area. That time is when they will have the best chance for quick service.

For a facility or OCS facility, an owner or operator must implement the TWIC program by the compliance date for the facility's COTP zone. These dates will be published in the Federal Register and publicized well in advance. So your workers might need TWICs well before the phase-in period ends. By then, all of your employees will have had an adequate chance to enroll before TWIC compliance. (You may require that your employees have a TWIC before we do.)

A vessel owner or operator must comply by September 25, 2008. If you do not comply with the TWIC program after the compliance date, you are subject to civil penalty action. We may also take further control and compliance measures, including suspending your operation.

Where to apply for enrollment

We want to make the enrollment process as easy as we can for your employees, workers, and for you. We will use both fixed and mobile enrollment centers. A fixed enrollment center stays open for a long term and any worker may use it. At the request of a large employer, we may open a short-term mobile enrollment center for the convenience of its employees.

At the end of the phase-in period, we will reduce the number of centers and staff. We will keep centers near the hubs of port facility and vessel activity. We will keep enough enrollment centers open to handle the following activities.

- New TWIC applicants.
- Replacements for lost, stolen, or damaged TWICs.
- TWIC renewals.

You can find our schedule for opening enrollment centers at www.tsa.gov/twic. Check often because the schedule may change. Remind your workers that they must pick up their TWICs from the enrollment center where they applied.

NVIC AND RELATED GUIDES

USCG uses *Navigation and Vessel Inspection Circulars* (NVICs) as a way to explain how it will enforce some of its rules and programs. A NVIC is not a rule. However, it is a tool for helping you comply with rules and programs and helping us be consistent. In Table 1, we say where you can find NVICs and other aids. The following NVIC may help you understand and comply with the TWIC program rules.

- NVIC No. 03-07 – *Guidance for the Implementation of the Transportation Worker Identification Credential Program in the Maritime Sector*.

Table 1: Information and Assistance Aids			
Source	**Who staffs it**	**Who it can help**	**How it can help**
Toll-free TWIC Call Centers (1-866-DHS-TWIC or 1-866-347-8942)	TSA Contractors	Transportation workers, facility and vessel owners and operators, and others who require assistance	Round-the-clock help with enrollment; lost, stolen, or damaged cards; PIN resets; scheduling enrollment appointments, locating the closest enrollment facility to an applicant; guiding applicants through the web-based pre-enrollment process
TSA Enrollment	TSA Contractors	Transportation workers and TWIC holders	TWIC enrollment and renewal; lost, damaged, or stolen cards; TWIC replacements; PIN resets; scheduling appointments
www.tsa.gov/twic	TSA	Transportation workers and TWIC holders	Enrollment Center locations and directions; Pre-enrollment
www.twicprogram.tsa.dhs.gov	TSA Contractor	Transportation workers, facility and vessel owners and operators, and others who require assistance	Enrollment Center locations and directions; Pre-enroll for a TWIC and schedule an appointment; Listing of required documentation to being to enrollment center; Frequently asked questions
USCG Help Desk (866-MTSA-AID or 1-866-687-2243)	USCG	Transportation workers; facility, vessel, and company security officers; facility and vessel owners and operators; the general public	Implementation and compliance questions regarding use of TWIC at MTSA regulated vessels and facilities. Enrollment and issuance questions will be forwarded to a contractor-maintained call center.
COTPs	USCG	Facility, vessel, and company security officers; facility and vessel owners and operators	Implementation and compliance questions regarding use of TWIC at MTSA regulated vessels and facilities in their COTP zone.
http://homeport.uscg.mil (Coast Guard's portal for sharing information with the public and security officers)	USCG	Transportation workers; facility and vessel security officers; facility and vessel owners and operators; the general public	TWIC FAQs, general information, news and events, and outreach sources; NVICs and Circulars about the TWIC program; portal for entering new hire's personal data and employer contact information
http://www.uscg.mil/hq/g-m/nvic/index00.htm	USCG	Facility, vessel, and company security officers; facility and vessel owners and operators	NVIC No. 03-07, *Guidance for the Implementation of the TWIC Program in the Maritime Sector* and related guidance

What the TWIC Program Means to You

If you are an owner or operator, a TWIC applicant, or TWIC holder, U.S. law says you *must* comply with Federal rules. Under the Maritime Transportation Security Act (MTSA) and the Security and Accountability for Every (SAFE) Port Act, the Secretary must establish rules to prevent an unauthorized person from getting into a secure area of a vessel or facility that has a security plan. We based the TWIC rules on these two laws. The laws require using a standard, biometric ID (also known as a "credential"), for access control to secure areas of vessels and facilities. We call that ID the "Transportation Worker Identification Credential" or "TWIC." To get a TWIC, an applicant must pass a Security Threat Assessment (STA). That assessment helps us decide if a person poses a risk to transportation security.

By September 25, 2008, every U.S. credentialed merchant mariner must have a TWIC. (Read the part of this guide titled, *Who Must Get a TWIC* to find out what you may accept as a valid merchant mariner ID before then.) Any other person who needs unescorted access to a secure area at a vessel or maritime facility must also have a TWIC by that date, if not earlier.

No one may go into a secure area unless you authorize it – even if the person has a TWIC. To be in a secure area, a person without a TWIC must be "escorted." That means the person must be with someone who has a TWIC or be "monitored" under our rules. Everyone in a secure area must have your permission to be there.

IS MY VESSEL OR MARITIME FACILITY COVERED?

If you own or operate a vessel we describe in 33 CFR 104.105, except for foreign flagged vessels, the TWIC program rules apply to you. Again, if you own or operate a foreign vessel, the TWIC program rules do not apply to you.

Who must be a U.S. Citizen on a U.S. Flagged Vessel
- Master
- Chief Engineer
- Radio Officer
- Officer in charge of a deck watch
- Officer in charge of an engineering watch

If you own or operate a U.S. flagged vessel, U.S. law says that only a U.S. citizen may serve in some positions. But this law does not apply for U.S. Offshore Supply Vessels (OSVs) and U.S. Mobile Offshore Drilling Units (MODUs) while they operate under a waiver in support of an OCS facility in foreign waters. When you operate under a waiver for one of these vessels, our laws let you hire foreigners as crew. As long as you operate under this waiver in support of an OCS in foreign waters, the TWIC rules do not apply. Your vessel has no secure area. But as soon as your vessel stops operating under the waiver, we consider it as having secure areas. You must follow the TWIC program rules.

If you own or operate a maritime facility described in 33 CFR parts 105 or 106, the TWIC program rules apply to your operation, unless your facility is located in the Commonwealth of Northern Marianas Islands. Facilities in the Commonwealth of Northern Marianas Islands do not have to implement the TWIC program but must continue to operate under all other requirements in 33 CFR Part 105.

WHAT A TWIC IS AND WHAT IT LOOKS LIKE

A TWIC is a standard biometric ID. It contains a numeric code. The code is associated with the TWIC holder's fingerprint template embedded in an electronic chip to link the card to the cardholder. The TWIC also has the person's photograph and special features on the surface to make it easy to tell if someone tampered with it. There are security features embedded in the card to protect any personal information. Security staff can tell if a TWIC is damaged or missing special features. These features make the TWIC hard to copy or change.

TWIC OR PERSONAL IDENTIFICATION

If a worker has no TWIC, that person must show security staff another ID to enter a secure area at your vessel or maritime

Must-have Traits for Other ID
- Be laminated or otherwise secure against tampering.
- Contain the holder's first and last name and any middle initial.
- Have a photo of the holder's face that shows how the person currently looks.
- Have the name of the issuing authority.

facility. That ID must come from you, a government authority, an employee union, or a trade association. These workers must be escorted. Some people do not need to have a TWIC for unescorted access to a secure area. To find out who these people are, read the part of this guide titled, *TWIC Basics*. It starts on page 10.

WHAT YOU MUST DO

To maintain security, you must control access to all secure areas at a vessel or maritime facility. Before you give someone unescorted access to a secure area, your security staff must positively verify their TWIC. Usually, this happens at an access control point to a secure area.

You *must* treat the TWIC as a visual ID badge. However, you *may* also ask for a fingerprint any time before giving someone unescorted access to a secure area. (Note that we do not *require* you to have a biometric card reader right now.) Our rules require that a person coming to your vessel or maritime facility must consent to screening or inspection for entrance into the secure area. A person who does not submit to this cannot board a vessel or OCS facility or enter a facility. You may ask a TWIC holder to use another ID that is linked to the TWIC.

People with Authority to Inspect a TWIC
- TSA
- Coast Guard
- DHS
- National Transportation Safety Board
- Federal, State, or local law enforcement officers.
- Owner or operator
- Owner or operator's security representatives

For example, your employees may have a company-issued ID card that they put through a scanner to enter your property. You may use that card for access control if you can tie it to the TWIC. The holder still must have the TWIC in his or her possession or near enough to get it within 10 minutes in case someone with authority wants to see it. We do not require the holder to wear the TWIC, but you may require it.

WHAT THE COAST GUARD DOES DURING AN INSPECTION

During an inspection or spot check, USCG may use handheld biometric card readers to check the TWIC. We use the card reader and the holder's PIN to match the worker's fingerprint to the fingerprint code on the TWIC. By doing so, we make sure the TWIC is real, that the holder is the rightful owner, and that TSA has not revoked it.

About Secure Areas and Escorting

Controlling access to secure areas is the core of the TWIC program. One way to control access is to keep people out unless they have the right ID. Another way is through following the rules for escorting in these areas.

Positive verification of the TWIC means:
- Comparing the holder's face to the photo on the TWIC.
- Checking that the TWIC has not expired.
- Examining the TWIC to make sure it is real and no one changed it.

SECURE AND RESTRICTED AREAS

A *secure area* is an area that has security measures in place or access control. For a facility, the secure area is generally any place inside the outer-most access control point. For a vessel or OCS facility, the secure area is generally the whole vessel or OCS facility.

A *restricted* area is a part of a secure area that needs more limited access and higher security. Under MTSA rules, you must designate some areas as restricted. For example, storage areas for cargo are restricted areas under our rules.

You must mark any secure area or restricted area clearly. Being in a secure area or restricted area without authorization is a breach of security and against the law.

ESCORTING

If someone does not have a TWIC and you give that person access to a secure area, that person must have a TWIC holder as an escort. "Escort" means different things in different operational

settings. "Escorting" could be having a TWIC holder stay with the person all the time while that person is in the secure area. "Escorting" also could be "monitoring" someone in the secure area if it is not also a restricted area. A proper escort under our rules means a TWIC holder must observe where the non-TWIC holder is and what he or she is doing. You must plan to respond quickly if a person goes in an area without authority. You also must plan for quick response if a person does something you have not authorized.

Quick-Response Measures
- Security guards
- Interoperable communications gear
- Suitable transportation
- Watchstanders working with a roving watch

Appropriate Escorting Ratio

In a secure area, that is not also a restricted area, you may have one TWIC holder to escort no more than 10 people without TWICs. If you want a TWIC holder to escort more than 10 people without TWICs, you must write to the COTP and request approval. We will approve any such request for a limited time only. But you must show you will increase other security measures for us to approve your request.

Monitoring

In a secure area that is not also a restricted area, you may monitor a non-TWIC holder in many ways. Among those could be one of the following.

- Closed-circuit Television (CCTV). You may use this system if there is a TWIC holder watching and operating the CCTV. The system must let your operator see if the monitored person goes to an area or engages in an activity without your authority.
- Other systems. You may combine security patrols, roving watches, automatic devices that detect intruders, or surveillance equipment. These are fine if they can ensure three things. The first is that a person under escort does only what you gave them authorization to do. The second is that the person stays in areas for which you gave authority. The third is that you can respond quickly if the monitored person does anything wrong.

Escorting In a Restricted Area

If the secure area *also is restricted*, the only right way a person without a TWIC could be there is with a TWIC holder. That TWIC holder must be near and able to see the person all the time he or she is in the restricted area.

Escorting a Newly Hired Employee

If a worker is a newly hired employee under our rules, escorting may be different. Look at the part of this guide titled, *Access for a Newly-Hired Employee.*

A Word About Areas on Maritime Facilities Immediately Beside Vessels

When a vessel visits your maritime facility, the vessel's crew commonly needs to work right beside their vessel (handling lines, taking draft readings, etc.). Some vessel crew may not have TWICs, or they may not be U.S. merchant mariners. Although the dock, pier, or platform the vessel is moored to is a secure and restricted area, you do not have to escort any of the vessel crew members who do not have TWICs while they work beside their vessel. However, if crew members who do not have TWICs need to go to another secure or restricted area away from their vessel, then they must be escorted.

PUBLIC, PASSENGER, AND EMPLOYEE ACCESS AREAS

A public, passenger, or employee access area may be on the vessel or facility. These areas are not part of the secure area and cannot be in a restricted area. The rules do not require people to have a TWIC to be in public, passenger, and employee access areas.

Public Access Areas

You may have workers at your facility who work only in areas open to the public. Do they need a TWIC for access to those areas? If this area is part of a facility that serves ferries or passenger vessels carrying more than 150 passengers other than cruise ships, you may designate it a public access area in your FSP. A public access area lets people walk through a facility to a vessel. Under our rules, people working in a public access area do not need a TWIC to be

there unless it is an individual whose primary duty is security. (If the facility serves a cruise ship, there are no public access areas. A worker must have a TWIC.)

Passenger Access Areas

You may have workers on a passenger vessel or ferry who work only in areas open to passengers. Do they need a TWIC for access to those areas? You may designate any area open to passengers on these kinds of vessels as a passenger access area. Some examples of this kind of area are vessel dining rooms, seating areas, parking decks, public restrooms, and bars. So if a worker holds a job such as a musician, wait staffer, or casino worker, that person may never enter an area that requires holding a TWIC. Under our rules, a TWIC is not needed to be in a passenger access area.

Employee Access Areas

You may have workers on a passenger vessel or ferry who work only in areas that support passenger access area activities. You may designate these kinds of areas as employee access areas. Some examples of employee access areas are vessel galleys, storage areas, dressing rooms, and food service areas. Your employees may go into any such area without a TWIC. A passenger cannot enter an employee access area. You may not designate an employee access area on a cruise ship.

A Word about Cruise Ships

If you own or operate a U.S. flagged cruise ship, you may not designate an employee access area on your cruise ship. Long cruise ship voyages mean more contact with passengers and more time to access vessel spaces. In turn, this contact and access mean a greater chance to create a Transportation Security Incident (TSI). A cruise ship employee must have a TWIC for unescorted access to every area other than a passenger access area.

TWIC Basics

Through the TWIC program, we want to make sure that the only people who get a TWIC are the ones who need it and have passed our STA. To get a TWIC, a person must be eligible to apply *and* must pass our STA successfully.

This part of the guide will help you understand who meets our standards for getting a TWIC. (The *Small Entity Guide for Applicants* has a complete section titled, *How to Apply for a TWIC*.)

This part of the guide also will tell you about the following topics.

- Compliance dates for having a TWIC.
- Your role in deciding who needs unescorted access to a secure area.
- Your responsibility for controlling access.

WHO CAN GET A TWIC?

Some people must get a TWIC, and some people can apply if they want to. All of these people must meet our standards to qualify and pay a fee to cover the cost of the process. But not just anybody who meets our standards can get a TWIC. Either we say a worker must have a TWIC or you say a worker must have one for unescorted access to a secure area.

There are some State and local authorities who we permit to get a TWIC if they believe they need one. In this part of *TWIC Basics*, we explain who is eligible to get a TWIC.

Who Must Get a TWIC

A person must have a TWIC if that person is a credentialed U.S. merchant mariner *or* a person who requires unescorted access to any secure area of a vessel or maritime facility subject to the TWIC program rules. So contractors and truckers might need a TWIC if you require that they have unescorted access to a secure area.

U.S. Credentialed Merchant Mariner holds a USCG-issued –
- Merchant mariner's license
- Merchant mariner's document
- Certificate of registry.

Even if our rules say someone must have a TWIC, remember that you decide who may enter a secure area on your vessel or maritime facility without escorting. Having a TWIC is not a *right* to unescorted access. (Tell your security staff to

inform workers if your vessel or maritime facility comes under the TWIC program.)

When Workers Must get a TWIC

The dates when workers must have a TWIC at a facility or OCS facility depend on when we require compliance in your COTP zone. For a vessel, workers must have a TWIC by September 25, 2008.

If you own or operate a facility, we will tell you at least 90 days before we require a TWIC for unescorted access in your COTP zone. Your compliance date will follow the "peak enrollment period" in your area– the period when workers have the best chance for quick service.

When we begin enrollment in a COTP zone, we will make sure we have convenient places for people to apply. We will tell you when we are beginning enrollment in your area. Remind your workers that applying early speeds up the process. Keep checking in your COTP zone so that you do not miss the enrollment or compliance dates.

On the date we designate for compliance in your COTP zone, a worker must have a valid TWIC to get unescorted access to a secure area of your property. We will work with you to provide notice of the compliance date.

For nearly 205,000 credentialed U.S. merchant mariners who must get a TWIC, enrolling may be hard because they move from place to place. These merchant mariners may apply for a TWIC at any time once enrollment starts. They may apply at any enrollment center. (Remind merchant mariners that they must pick up the TWIC at the enrollment center where they apply.)

Merchant Mariners

Before September 25, 2008, here are documents you can accept instead of a TWIC.

- Merchant Mariner Document (MMD)
- Merchant Mariner License and a picture I.D.
- Certificate of Registry and a picture I.D.

You may permit a merchant mariner without a TWIC to have unescorted access to secure areas until September 25, 2008, even if the compliance date for your COTP zone has passed.

To be in a secure area without an escort –

- The person must have a TWIC, and
- You must authorize the person to be in that secure area without an escort.

In fact, during that time, these people may be escorts under the TWIC program if you allow it. They must use one of the alternate identity documents we spell out in the rules. (See the box headed *Merchant Mariners*.) However, we encourage merchant mariners to apply early for their TWICs.

For long-haul truckers, their work also may take them to secure areas in more than one COTP zone. They must have a TWIC for unescorted access to a secure area in any COTP zone where compliance has begun. This is true even when that trucker comes from a COTP zone where the compliance date has *not* been reached and is going to a COTP zone where compliance *has* begun.

(For a newly hired employee, there are special provisions for access to a secure area. A worker comes under these special rules between the time of application for a TWIC and the time he or she gets a TWIC from TSA if compliance has begun for the facility or vessel where he or she works. Read the part of this guide titled, *Access for a Newly-Hired Employee*.)

People You Should Encourage to Obtain a TWIC

What if some of your workers often are in a secure area as part of their work? It would probably be best for you and them if these workers had a TWIC. We expect such individuals to get a TWIC instead of being under escort over a long period of time. Here are some of the kinds of workers in this group.

- Vessel crew (other than U.S. credentialed merchant mariners).
- Longshoremen.
- Drayage truck drivers who handle cargo near a vessel.
- Facility employees working in a secure area.

Federal Officials; State and Local Law Enforcement Officials; and State and Local Emergency Responders

Some people do not need to have a TWIC at all for unescorted access to a secure area.

Federal officials

A Federal official must present an agency-issued, HSPD-12 compliant card for unescorted access to a secure area. (Through a directive from the President, Federal employees, contractors and affiliates must undergo a standard identity verification process and hold a specific personal identification card – the HSPD-12 compliant card.) If that official's agency has not issued this kind of identity document, he or she may use the agency's official credential for unescorted access to secure areas until the agency issues an HSPD-12 compliant card.

State or local law enforcement officials

A State or local law enforcement officer probably had some type of background check before starting the job. These officers may have unescorted access to secure areas without a TWIC when they are there for official business. You must let them enter the vessel or maritime facility at any time and without delay or obstruction for official business. Still, we encourage these officers to get a TWIC if they need access to any secure area as a regular part of their duties.

State or local emergency responder

A State or local emergency responder may have unescorted access to a secure area *during an emergency*. We know that not all emergency responders are State or local officials. Still, *in an emergency*, a responder may need unescorted access even to a secure area. If an emergency responder is not a State or local official, we encourage that person to get a TWIC. We also encourage State or local emergency responders to get a TWIC if access to a secure area is a regular part of their duties.

Note that any one of the groups we just talked about may use unescorted access authority only for official duties. Also, in an emergency, these groups must follow your approved vessel and facility security plans.

Area Maritime Security Committee (AMSC) Members

An AMSC member who needs access to sensitive security information (as determined by the COTP) must hold a TWIC, have passed a comparable STA, *or* pass a name-based terrorist check from TSA.

YOUR RESPONSIBILITY AND AUTHORITY TO CONTROL ACCESS

On request, a TWIC holder must show the TWIC to–

- An authorized TSA, USCG, DHS, or NTSB representative.
- A Federal, State, or local law enforcement officer.
- Your authorized security staff.

We said that you must control access to a vessel or maritime facility. So a person who comes to an access control point must show a TWIC to your authorized security staff. Also, if an official with inspection authority asks, a TWIC holder must present the TWIC for inspection. Remember, too, that you make the rules for who can have unescorted access.

What if a person presents a TWIC and your security staff suspects the TWIC is not real? What if the TWIC shows signs of tampering? You must plan how you will handle situations like these. We talk about this in the part of this guide titled, *Your Enforcement Obligations*. It starts on page 20.

Authority to Incorporate TWIC into an Existing Physical Access Control System

Our rules let you use an access control system you already have. That means workers could be using your vessel or maritime facility access card to get unescorted access to a secure area. Still, they must have a TWIC because the access card must link any card you issue to the TWIC.

WHO IS ELIGIBLE TO HOLD A TWIC

A worker who is a U.S. national may hold a TWIC. A worker who is not a U.S. national can hold a TWIC if that person is in one of the groups identified in our rules. Table 2 shows who may hold a TWIC and some of the laws that apply.

Table 2: Who May Hold a TWIC
General
National of the United States
U.S. lawful permanent resident
Refugee admitted under 8 U.S.C. 1157
Alien granted asylum under 8 U.S.C. 1157
Alien in a valid M-1 nonimmigrant status who is enrolled in the U.S. Merchant Marine Academy or a comparable State maritime academy
Lawful Nonimmigrant Status
Admitted under the Compact of Free Association between the U.S. and the Federated States of Micronesia, the U.S. and the Republic of the Marshall Islands, or the U.S. and Palau
Unrestricted authorization to work in the U.S., unless you are an alien whose status is one of the following: S-5, S-6, K-1, K-2
Alien with one of these restricted authorizations to work in the U.S.: C-1/D Crewman Visa; 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; TN North American Free Trade Agreement
A complete list of lawful nonimmigrant statuses may be obtained from the TSA website www.tsa.gov/twic or by calling the TWIC Call Center at 1-866-DHS-TWIC.
CDL Holder
Licensed in Canada or Mexico and admitted to the U.S. under 8 CFR 214.2(b)(4)(i)(E) to conduct business in the U.S.

WHAT CAN DISQUALIFY SOMEONE FROM GETTING A TWIC

A person's status can make him or her ineligible to get a TWIC without a waiver. Some status conditions can prevent a person from getting a TWIC at all.

One status we look at is the criminal records status. We call a disqualifying criminal offense "permanent" or "interim" to indicate how far back we will look at a person's criminal history in making a decision on a TWIC. Some offenses are disqualifying no matter how long ago they occurred (permanent disqualifying offenses) and some are disqualifying if the conviction occurred within the previous 7 years, or release from incarceration occurred within the previous 5 years (interim disqualifying offenses).

A worker with certain permanent disqualifying criminal offenses may be unable to get a TWIC at all. Workers with other criminal offenses, a certain mental incapacity status, or a certain immigration status may be unable to qualify for a TWIC through the regular process. They would have to apply for a waiver.

If the STA process leads us to decide that a person is a security threat, we will not issue a TWIC.

Permanent Disqualifying Criminal Offense

A "permanent disqualifying criminal offense" is an offense we will consider whenever we conduct an STA – even if the offense was a long time ago. What if an applicant has a record of a permanent disqualifying offense? Table 3 shows these offenses. If a worker's record has one of the first four listed in Table 3, that worker cannot get a TWIC and cannot get a waiver. If a worker has any of the other crimes listed, he or she should apply for a waiver.

The *Small Entity Guide for Applicants* covers this topic in *Applying for a Waiver*. Refer your

workers to that guide for more information on how these offenses affect getting a TWIC.

Table 3: Permanent Disqualifying Criminal Offenses	
1	Espionage or conspiracy to commit espionage.
2	Sedition or conspiracy to commit sedition.
3	Treason or conspiracy to commit treason.
4	A federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable State law, or conspiracy to commit such crime.
5	A crime involving a transportation security incident.
6	Improper transportation of a hazardous material under 49 U.S.C.5124, or a State law that is comparable.
7	Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipment, transport, import, export, storing, or dealing in an explosive or explosive device. An explosive or explosive device is an explosive or explosive material defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f). But more things than these could be an explosive or explosive material.
8	Murder.
9	Threatening, or maliciously conveying false information knowing it to be false, about delivering, placing, or detonating an explosive or other lethal device in or against a place of public use, a State or government facility, a public transportation system, or an infrastructure facility.
10	Violating the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. 1961, et seq, or a comparable State law, where one of the predicate acts found by a jury or admitted by the defendant is one of the crimes listed in this Table.
11	Attempt to commit the crimes in 1 through 4.
12	Conspiracy or attempt to commit the crimes in 5 through 10.

Interim Disqualifying Criminal Offenses

Has the person committed an offense in Table 4? If so, the applicant should check conviction and imprisonment dates to figure out if he or she has this kind of offense during the look-back period. Refer your workers to the *Small Entity Guide for Applicants* for more information on how these offenses affect getting a TWIC.

Even if an applicant has no record of a disqualifying criminal offense, that worker may be wanted for one of those offenses. The person might be formally accused and waiting for a trial. The person might be under warrant for arrest. These workers cannot get a TWIC.

Table 4: Interim Disqualifying Criminal Offenses	
1	Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon can be one defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5 845(a), or an item on the U.S. Munitions Import List at 27 CFR 447.21. But more things than these could be a firearm or other weapon.
2	Extortion.
3	Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering relates to a crime that is a permanent or interim disqualifying offense. For TWIC, passing a bad check or welfare fraud is not dishonesty, fraud, or misrepresentation.
4	Bribery.
5	Smuggling.
6	Immigration violations.
7	Distributing a controlled substance, possessing it with intent to distribute, or importing it.
8	Arson.
9	Kidnapping or hostage taking.
10	Rape or aggravated sexual abuse.
11	Assault with intent to kill.
12	Robbery.
13	Fraudulent entry into a seaport as described in 18 U.S.C. 1036, or a comparable State law.
14	Violating RICO, 18 U.S.C. 1961, *et seq*., or a comparable State law. Do not count a RICO violation that is a permanent disqualifying offense.
15	Conspiracy or attempt to commit any of the crimes in Table 4.

Immigration Status

Immigration status may prevent a person from getting a TWIC. (Table 2 shows legal statuses eligible to hold a TWIC.) Or a TWIC holder's immigration status might change. For example, what if a permissible status expires?

A worker should not apply for a TWIC in the first place if the U.S. has ordered him or her to leave or is trying to make that person leave under U.S. immigration laws. Refer your workers to the *Small Entity Guide for Applicants* for more information on how immigration status affects getting a TWIC.

If we issue a TWIC to an immigrant, you have special responsibilities. Look back at Table 2 in the row that reads, *Alien with one of these restricted authorizations to work in the U.S*. If a person with the status we describe in that row leaves your employ for any reason, you must tell TSA within 5 business days of the event. That person should give you his or her TWIC. If possible, you must give the TWIC to us.

Mental Incapacity

An applicant may have a "mental incapacity" that stops the person from getting a TWIC. A mental incapacity under our rules is a condition where a court or other lawful authority finds a lack of mental capacity. A worker also may be in this group if a court or other lawful authority commits him or her involuntarily to a mental health facility. These workers should apply only under the waiver provisions. Refer your workers to the *Small Entity Guide for Applicants* for more information on how mental incapacity affects getting a TWIC.

If your worker or employee is in one of the groups we just talked about, we could decide that he or she poses a security threat. On the other hand, an applicant may give us information that helps us decide to grant a waiver.

Security Threat

Even if an applicant is not in one of the groups we just talked about, after we do an STA, we

may decide that the person poses a security threat or may pose a security threat. That is, we may find that the person has a connection with terrorist activity. We could decide this after we check immigration status, criminal history, and other information. Such a person would not get a TWIC.

If we decide an applicant should not get a TWIC, that worker could appeal our decision to a higher DHS authority or an administrative law judge. We talk about that in the *Small Entity Guide for Applicants* under, *Waivers* and *Appeals*.

ACCESS FOR A NEWLY-HIRED EMPLOYEE

Who May Use the New Hire Provision

You may use the new hire access authority for your vessel if the vessel's Certificate of Inspection (COI) may show a total vessel crew of not more than 10. The "vessel crew" is all credentialed merchant mariners. A worker is not "vessel crew" if the COI lists him or her as a "person in addition to crew, passenger, or other crewmember."

You may use the new hire access authority for your facility if there are not more than 25 employees in the work unit where you assign the new hire. (A work unit is a subset of the larger organization. Identify a work unit by its geographical location and the extent of its operations. The employees in such a unit work regularly and closely together.)

Only 25 percent of your total vessel crew or facility employees can be under the new hire provision at any one time. This means that if you have 4 people total as your vessel crew, only one person can be working under the new hire provision. If you have 19 employees on your facility, then you can have up to 5 people working under the new hire provision (we allow you to round up to the nearest whole number when calculating the 25 percent of vessel crew or facility employees).

What the New Hire Provision Allows You to Do

You might need an employee's services in a secure area between the time that employee applies for a TWIC and the time TSA issues the TWIC. In a case like this, the TWIC rules let you use that employee in a secure area without a TWIC. We must do a name-based security check before you can treat the employee as a new hire under our rules. When you get our positive clearance through Homeport, USCG's secure web portal, a TWIC holder may "accompany" – rather than escort – the new hire. "Accompanying" is a different security measure from escorting. The new hire may not work alone. But he or she may work with a TWIC holder in the same general space.

In deciding if your procedures to accompany a new hire meet the TWIC rules, USCG uses the following guidelines.

- Crew or staff size.
- Number of TWIC holders.
- Other appropriate factors.

The new hire rules apply to *your employees only*. You may not use the new hire rules for a contractor, a self-employed worker, or another company's employee. You may not use the new hire rules for a company, facility, or vessel security officer, or anyone whose primary duties are security-related. Only a TWIC holder may have a position where the primary duty is security.

Also, you must decide that your business would suffer an adverse impact unless the new hire starts working in a secure area before he or she has received a TWIC.

What the New Hire Must Do

You may consider using the new-hire rules for a person who meets the following profile.

- The person applied for a TWIC under our rules and paid all the fees.
- The person is *not* applying for a waiver and says so in writing.
- The person has another ID that has all the traits we require. Look at the box in this guide titled, *Must-have Traits for Other ID* for a description of other IDs we will accept. It is on page 7.

What You Must Know About the New Hire

You must have no reason to believe the new hire will not pass an STA. For example, what if you knew something that made you think immigration status would disqualify a person

from getting a TWIC? You would have reason to believe we would deny the person a TWIC. We do not expect you to do a search to find reasons why we may deny the application. Rather, use information you have. Maybe something happened in the interview. Maybe you learned something from a job application or a company background check.

Did the COTP tell you that the person is a security threat? If the answer is yes, you cannot use our new hire rules for this person.

How to Use the New Hire Provision

If the new hire has the above requirements and you have no reason to believe we will not give him or her a TWIC, follow these steps to use the new hire access authority.

- Enter the right data in Homeport for TSA's name-based security check.
- Wait for our positive name-check clearance.
- Observe the right ratio for TWIC holders to new hires.
- Use the new hire authority only as long as the TWIC rules allow.

Enter the right data in Homeport for TSA's name-based security check

We talked about USCG's Homeport website (http://homeport.uscg.mil) in the part of this guide titled, *Where to Go for Information and Assistance*. To use the new hire provision, you or your security officer must register in Homeport. Then, for the new hire provision only, you may use Homeport to ask for the status of our name-based security check on your new hire.

Enter this information for a new hire
- Full name
- Birth date
- Employer point of contact
- 24 hour contact information

You or your security officer must enter information in Homeport *exactly* as the applicant entered it at the enrollment center. If you do anything differently, Homeport cannot return the new hire entry. For example, if the new hire entered her name as "Dorothy" and you enter it as "Dot," we will not find her in the Homeport system. You would have to reenter the information.

Wait for our positive name-check clearance

We can complete the name-based check in three days or less. If the new hire entered his or her Social Security Number (SSN) at the enrollment center, you can include that data in Homeport. We can process the name-check faster with the applicant's SSN. But if the applicant did not input an SSN at the enrollment center, your giving it to us will not speed things up.

Observe the right ratio for TWIC holders to new hires.

In general, once you get our positive name-check clearance, you can let the new hire into a secure area under the following conditions.

- If you have four or more total employees, not more than 25 percent of your employees are using new hire access. (Number of employees x 0.25. Round product to the nearest whole number.)
- If you have fewer than four total employees, no more than one are using new hire access.
- Everyone is following your security measures for access control and monitoring according to your USCG security plan.
- If a new hire works in a restricted area, you "monitor" the new hire as we describe in the part of this guide titled, *Escorting*. It starts on page 8.

Use the new hire authority only as long as the TWIC rules allow.

You can use this new hire authority for 30 consecutive days from the date a worker enrolled in the TWIC program. If TSA does not act on the new hire's application within that time, the COTP may approve an extended period of another 30 days.

Under the TWIC rules, you do not have to keep a record to track when a worker's new hire access ends. However, you are responsible for ensuring the 30-day time limit is not exceeded. We suggest that you set up a process to list your new hires and track when their new hire access ends.

TWIC Security Requirements

Since 2003, USCG rules have had security measures that you must describe in detail in your VSP, FSP, or ASP. The TWIC program rules add the following new measures, but you do not need to add them to your plan right now.

GENERAL OWNER/OPERATOR SECURITY MEASURES

You must tell your employees about their TWIC program responsibilities. These include how and when to apply for a TWIC, the duty to maintain a TWIC, and the duty to tell TSA anything that makes an employee not eligible for a TWIC. Also, you must tell your employees of their duty to tell TSA if something happens to invalidate a TWIC, like if their TWIC is lost, stolen or damaged.

- You must ensure access control for any secure area according to the TWIC rules. This control includes making sure that only TWIC holders have unescorted access to this area, describing what an escort should do if there is a security breach, and marking any secure area.
- You must let everyone on your vessel or at your facility know where there are secure or restricted areas or passenger, public, or employee access areas – whichever applies.
- You must have a plan that meets our rules for dealing with any worker who reports a TWIC as lost, damaged, or stolen.
- If you have new hires, or if you expect to, you must have a plan that meets our rules for dealing with them.

SECURITY PERSONNEL

Since 2003, you also have had security officers for your company, for each vessel, or for your maritime facility. Under the TWIC program rules, these officers must apply for and maintain a TWIC. The CSO, FSO, and VSO must know about the TWIC rules and ensure you have a TWIC program. These officers must ensure your operation follows that program correctly. Other security staff must know about the TWIC program, too.

> See *Owner or Operator* at 33 CFR §§ 104.200 (vessels), 105.200 (facilities), and 106.200 (OCS facilities).

TWIC Program Knowledge for Other Staff

You must make sure that all of your workers know about any part of the TWIC program that concerns them. Your workers can get this knowledge through training or on-the-job experience.

ACCESS CONTROL RESPONSIBILITIES

You have learned that you must use the TWIC for access control in a secure area. Here, we talk about specific security measures you must take for access control because of the TWIC program.

Since 2003, our rules state that a vessel or maritime facility owner or operator must take measures to control access. The TWIC program rules add the following new measures.

- You must make sure that the only unescorted people in a secure area are TWIC holders who have your authorization to be in those areas.
- You must say where you will apply TWIC access control measures for each MARSEC Level.
- You must say how your security staff will identify non-TWIC holders and escort them under our rules.
- For each MARSEC Level, you must say how your security staff will identify people with authorization to be in a secure area and those without authorization to be in a secure area.
- If you have an access control system that uses access cards other than the TWIC, you must make sure that your system can be configured so that only people who hold valid TWICs are granted unescorted access.
- Your security staff must implement the TWIC program appropriately at every MARSEC Level.

How You Must Implement the TWIC Program

You must make sure you, your workers, and your security staff implement the TWIC program according to our rules. Note that a facility or OCS facility owner or operator must implement the TWIC program by the compliance date in the facility's COTP zone. A vessel owner or operator must implement the TWIC program by September 25, 2008. This part of the guide briefly explains how you do that.

TWIC Inspection

A worker must present a TWIC for inspection if that person wants unescorted access to a secure area. The worker also must have your authorization to be in the area.

What it means to "inspect"

- Match the TWIC photo to the person who presents it.
- Verify the TWIC date is valid.
- Check for signs that someone changed the TWIC.
- Check to make sure the TWIC is real.

Lost, Damaged, or Stolen TWIC

A worker may claim he or she cannot present a TWIC because it has been lost, damaged, or stolen. Do you or your security staff know that the worker had a valid TWIC? Did you give that worker authorization for unescorted access before? Have they reported the TWIC lost, damaged, or stolen to TSA? If you answer "yes" to all three questions, you may let that person have unescorted access to a secure area for 7 days from the day when the individual reported the TWIC lost, damaged, or stolen to TSA.

Before you can use this authority, you or your security staff must have *no* reason to be suspicious about the claim. The person must show you another ID like the ones we describe in the box titled, *Must-Have Traits for Other ID*.

What if a worker cannot present the TWIC for some other reason? Can you give that person unescorted access authorization? No, you cannot. If a person neither has a TWIC nor meets the profile we just described in this part, he or she must have a TWIC-holder escort while in a secure area.

Discipline

You must have disciplinary measures to prevent fraud and abuse.

Coordinating Access Control Measures

If it is possible, you should coordinate your TWIC access control measures with access control measures at any other vessel, maritime facility, or transportation conveyance with which you interface.

What you must do about your Vessel or Facility Security Plan

VSP

You may change your plan now if you choose to show the passenger or employee access areas. But if USCG approved your VSP before March 26, 2007, we do not require that you amend your VSP right now. You can wait until the next time you submit your plan for review.

If your vessel has any passenger or employee access areas, you must show which areas you classify in this way. You must keep a visual representation of these areas on board with the plan we approved, but you do not have to submit that representation to USCG until you submit your plan.

FSP

For a facility, the TWIC program rules should apply only in areas with a maritime transportation link. If your current FSP covers more than the maritime transportation related part of your facility, you can change your plan right now. You must continue to cover the whole facility in your security plan. But you may limit the TWIC program to those areas related to maritime transportation. You must apply to the COTP for permission to change your plan in this way.

The kinds of facilities that may apply for this permission include the following.

- Refineries.
- Chemical plants.
- Factories, mills, power plants.
- Smelting operations.

The kinds of facilities that cannot take advantage of this provision have major maritime transportation links such as container yards and passenger terminals.

Your Enforcement Obligations

Picture this. A person with a TWIC presents it at your vessel or maritime facility, but something appears not right. The security person at the access control point suspects that the TWIC itself is false. Maybe the TWIC looks like someone changed it. What should happen next?

First, if possible, have security personnel stop the person from entering a secure area without an escort. Presenting a fake or changed TWIC is a suspicious activity.

If we revoke a TWIC for any reason, we list the credential on a "hotlist" of revoked cards. Your access control measures may include comparing the TWIC with the hotlist. If a worker presents a TWIC we have revoked, your staff should make note of it and deny access.

Second, tell your security personnel to ask for one of the other identity documents we describe in *Other Personal Identification*. Check that ID, too. Does it look real? Does it look like someone changed it? Get the holder's name, address, and contact information. Make sure security keeps a record of this information.

Third, one of the security personnel should call the COTP. The caller should tell the duty officer the following.

- That someone presented a TWIC that looked false or changed.
- The name on the TWIC and on any other ID.
- A description of what makes the TWIC seem suspicious.

Your security personnel should do what the duty officer at the COTP office says. In some cases, this may include waiting for local law enforcement, USCG, or other authorized officials to arrive on scene.

If the duty officer says USCG will come over to get the TWIC, ask the TWIC holder to wait at the access control point. But make sure your security staff knows not to try physically restraining the TWIC holder. *State law varies on whether you have authority to detain the person.*

A Federal official cannot give you authority to take law enforcement action. You do not have authority to confiscate a TWIC. Only a Federal official may do that.

If conducting checks using electronic readers, security staff at your vessel or maritime facility may find the TWIC holder does not match the biometrics stored on the electronic chip (fingerprint code), or the status shows "invalid" for that TWIC. Although this failure is suspicious, there are many reasons why this could happen. It could be that TSA revoked the TWIC, that the TWIC is fake, or that someone changed the card presented. But the match or validation could fail for one of the following innocent reasons.

- The holder forgot his or her PIN.
- There is a false negative reading between the TWIC and the reader.
- There is a card reader error.

But if your security staff believes something is a "suspicious activity," you must make sure that someone reports that fact according to your existing procedures. For the TWIC program, a suspicious activity could look like any of the following.

- In the space of a week, different holders present TWICs that appear fake or changed in the same way.
- At different access control points, the same person tries using the same suspicious-looking TWIC.
- Your security staff encounters many TWICs that look different from each other or from what they should look like.

Your security staff must report to the COTP every incident of a person presenting a fake TWIC.

Conclusion

We think the TWIC program strikes a balance between these three goals.

- Enhancing security through using a secure, common ID to manage individual access to secure areas of the transportation system.
- Facilitating commerce through an identity management system that maintains, or improves worker access to transportation facilities.
- Protecting privacy by collecting as little personal data as necessary, putting that data on a secure ID, and preventing unauthorized disclosure.

We hope this guide helps you understand this important program and how to comply with it.