

Transportation Worker Identification Credential (TWIC)

Application to Facilities

AAPA Conference Call

June 4, 2007



Transportation
Security
Administration

*U.S. Department of
Homeland Security*
**United States
Coast Guard**



Highlights of Presentation

- TWIC Rulemaking Status
- Applicability
- Enrollment Process
- Credential Characteristics
- TWIC Fees
- DHS Agency Responsibilities
- Security Threat Assessment
- Disqualifying Offenses
- Program Plans for Moving Forward
- List of Final Rule Differences from the NPRM



TWIC Rulemaking Status

- In response to comments received on the joint TSA/CG Notice of Proposed Rule Making (NPRM) published 22 May 2006, we divided the TWIC program into two separate regulatory projects.
- The TWIC Final rule was posted on the TSA and Coast Guard web sites 1 January 2007 and published in the Federal Register 25 January 2007.
- The requirement to purchase and use TWIC readers will be addressed in a a second rulemaking.
- The public will have ample opportunity to comment on the technology and access procedures we propose in the second rulemaking.



Applicability

MTSA requires TWIC for:

- All individuals who require unescorted access to secure areas of MTSA regulated vessels, facilities, and Outer Continental Shelf (OCS) facilities, which includes but is not limited to longshoremen, truck drivers, vendors, facility/vessel employees, maintenance personnel, train crews, etc.
- All USCG credentialed merchant mariners
- Initial estimates were that ~750,000 maritime workers will require a TWIC. Actual number is expected to be much greater.



Enrollment Process

Pre-enrollment

- Web-based or phone
- Recommended, but not mandatory
- Will reduce time at enrollment center if completed beforehand

Enrollment

- Will have enrollment centers located throughout the country during the enrollment period
- At the enrollment center the applicant provides biographic information and identity verification documents
- A ten-fingerprint scan and digital photo are taken
- All information is encrypted and transmitted to the central TWIC system for processing



Enrollment Process (continued)

Security Threat Assessment (STA)

- Conducted by TSA
- Upon successful completion of the STA the TWIC is personalized by the centralized card production facility and shipped to the applicant's enrollment center
- Applicant will be notified when the credential is ready to be picked up

OR

- Applicant will be notified if he/she may be disqualified and of his/her appeal and waiver rights

Credential Pick-Up

- Applicant returns to enrollment center to claim credential for use at MTSA regulated vessels, facilities, and OCS facilities



Credential Characteristics

Smart Card-Based

- Supports off-line and on-line biometric authentication — no need to connect to a central database when authenticating
- Robust enough to support fingerprint templates and photograph, as well as future biometrics
- Supports future technology applications for additional capabilities
- Supports multiple levels of authentication
 - Something you have—the credential
 - Something you are—the biometric
 - Something you know—the Personal Identification Number (PIN)



TWIC Fees: (Note: Fees will be posted in a subsequent Federal Register notice)

<u>TWIC Enrollment Category</u>	<u>Fee Level</u>
Standard TWIC Enrollment	\$137.25
Hazmat/Mariner/FAST TWIC Enrollment	\$105.25 ¹
Lost/Damaged Card Replacement	\$36 ²

- TWIC user fees must fully offset program costs
- Standard user fee charged to applicant will cover:
 - Enrollment
 - Threat assessment and adjudication, including appeals and waivers
 - Card production
 - TSA program and systems costs

¹ Does not include FBI's Criminal History Records Check (CHRC) and TSA's related adjudication costs

² Does not include FBI's CHRC, TSA's threat assessment, and estimated enrollment costs; This fee may increase to \$60 and public comment is requested in Final Rule



DHS Agency Responsibilities

- TSA Responsibilities

- TWIC enrollment
- Security threat assessment and adjudication
- Card production
- TWIC issuance
- Appeal/waiver for TWIC denials
- Technology/TSA system management

- USCG Responsibilities

- Enforce use of TWIC at MTSA regulated vessels, facilities and OCS facilities
- Conduct biometric checks as part of vessel and facility compliance inspections



TWIC Security Threat Assessment

- Criminal History Records Check
 - Fingerprint and Name / Biographic-Based
 - Permanent Disqualifying Offenses
 - Interim Disqualifying Offenses

- Legal status
 - U.S. citizen or National
 - Lawful permanent resident
 - Refugees, asylees, and certain others with restricted & unrestricted employment authorization

- Intelligence/Terrorism Check



Disqualifying Offenses

(a) Permanent disqualifying criminal offenses -- Unlimited look back

- (1) Espionage or conspiracy to commit espionage
- (2) Sedition or conspiracy to commit sedition
- (3) Treason or conspiracy to commit treason
- (4) A crime listed in 18 U.S.C. Chapter 113B—Terrorism or conspiracy to commit such crime
- (5) A crime involving a TSI (transportation security incident)
- (6) Improper transportation of a hazardous material
- (7) Unlawful possession, use, sale, distribution, manufacture, purchase...or dealing in an explosive or explosive device
- (8) Murder
- (9) Threat or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of 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) Certain RICO (Racketeer influenced and Corrupt Organizations) Act violations (in which the predicate act is one of the permanently disqualifying crimes)
- (11) Conspiracy or attempt to commit the crimes in this paragraph (a)(5)-(a)(10)



Disqualifying Offenses (cont.) (as per Final Rule)

(b) Interim disqualifying criminal offenses -- Conviction within 7 years, or release from incarceration within 5 years of application, includes wants & warrants associated with crimes

- (1) Unlawful possession, use, sale, manufacture, purchase, distribution...or dealing in a firearm or other weapon
- (2) Extortion
- (3) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering
- (4) Bribery
- (5) Smuggling
- (6) Immigration violations
- (7) Distribution, possession w/ intent to distribute, or importation of a controlled substance
- (8) Arson
- (9) Kidnapping or hostage taking
- (10) Rape or aggravated sexual abuse
- (11) Assault with intent to murder
- (12) Robbery
- (13) Lesser Violations of the Racketeer Influenced and Corrupt Organizations Act
- (14) Conspiracy or attempt to commit crimes in this paragraph (b)



Secure Area

- **A secure area is defined as “the area over which an owner/operator has implemented security measures for access control” to reduce the probability of a TSI.**
- The secure area is the entire area within the outer-most access control perimeter of a facility, with the exception of public access areas, and encompasses all restricted areas. The secure area is bound by the fence line or other barrier, waterfront, and gates, which also provide access to the secure area.
- Facilities containing both a maritime transportation portion and a non-maritime transportation portion may voluntarily request a definition of their secure area through an FSP amendment.
 - E.g. refineries, chemical plants, mills, power plants, factories, etc.



Escorting

- **“Escorting” means ensuring that the escorted individual is continuously accompanied while within a secure area in a manner sufficient to observe whether the escorted individual is engaged in activities other than those for which escorted access was granted.**
- This can be accomplished through monitoring or physical, side-by-side accompaniment.
- 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.
- Accompanied access is a term reserved for new hires only. A new hire may be considered accompanied in their work area as long as the criteria listed in the NVIC are met (vessel/work unit size, % of employees that are new hires, etc.)



Escorting (cont.)

	SECURE AREAS THAT ARE NOT ALSO RESTRICTED AREAS	PORTIONS OF SECURE AREAS THAT ARE RESTRICTED AREAS * *AS DEFINED IN FSP OR VSP
TWIC HOLDERS	UNESCORTED	UNESCORTED
LOST, STOLEN OR DAMAGED TWICS	UNESCORTED ACCESS UP TO 7 CONSECUTIVE DAYS	UNESCORTED ACCESS UP TO 7 CONSECUTIVE DAYS
NON-TWIC BUT NEW HIRES	ACCOMPANIED ACCESS	ACCOMPANIED ACCESS
NON-TWIC	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 18 MONTH TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL	UNESCORTED ACCESS DURING 18 MONTH TWIC PHASE-IN PERIOD WITH OTHER CREDENTIAL
FOREIGN MARINERS	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TO 10 RATIO) OR MONITORING	ESCORTED – SIDE-BY-SIDE ACCOMPANIMENT (1 TO 5 RATIO)



New Hire Provision

- **Provision allows newly hired direct employees to work while waiting for issuance of their TWIC**
- **Employer must apply for provision via HOMEPORT after employee has completed TWIC enrollment**
 - **Information must be entered exactly as given at enrollment center for HOMEPORT to match to enrollment record**
 - **Owner/Operator/CSO/FSO/VSO will receive status of new hire within 3 days of enrollment**
 - **Once cleared status is given, new hire may have “accompanied” access for 30 days with an additional 30 days at COTP discretion**
 - **Accompanied access is described in NVIC, encl 3**



Future Milestones – Deployment & Compliance

Vessels and Mariners will have a compliance date of 25 Sept 2008.

- **Facilities will have a phased-in compliance, based on COTP zone.**
 - **Deployment schedule is forthcoming.**
 - **Dates announced in Federal Register & publicized locally.**
 - **Mariners can gain unescorted access to facilities before 25 Sept 2008 by showing MMD, License/ID, or COR/ID.**
- **Initial enrollment and issuance will be completed by 25 September 2008. This will be the date for nationwide compliance for vessels, facilities and mariners.**

Type of operation	Compliance Date
Vessels (33 CFR 104)	25 SEP 08
Facilities (33 CFR 105)	by COTP zone
OCS Facilities (33 CFR 106)	by COTP zone
Merchant Mariners	25 SEP 08



Program Plans for Moving Forward

- Lockheed Martin awarded the contract to operate and maintain the TWIC system and provide enrollment services.
- Rollout goal: issue credentials to all maritime workers and merchant mariners requiring unescorted access by September, 2008.
- Finalize specifications for a contactless biometric TWIC reader in preparation for a follow-on TWIC reader rulemaking.
- Conduct pilot tests of TWIC contactless biometric readers and credential validation processes in preparation for a follow-on TWIC reader rulemaking.



Final Rule Differences from NPRM

	Topic	NPRM	Final Rule
1	Access Control	Visual identity badge and reader (w/ biometric verification and validity check at facility/vessel based on MARSEC level)	Visual identity badge that must be presented to gain unescorted access secure areas; also Coast Guard conducts periodic validity checks
2	Escorted Access	Defined	Definition modified to clarify that in restricted areas (33 CFR 101.105), escort means physical accompaniment; outside restricted areas, escort may consist of monitoring
3	New direct hires	Not granted unescorted access to secure areas until successful completion of security threat assessment and card issuance	Permitted to have access for 30 consecutive days if employer receives approval from TSA w/ add'l 30 days after approval from COTP
4	Passenger access area	Defined only for certain vessels (passenger, ferries, cruise ships)	Passenger access area remains and employee access area for certain vessels added (employee access areas do not apply to cruise ships)



Final Rule Differences from NPRM (continued)

	Topic	NPRM	Final Rule
5	TWIC Addendum to Security Program & Recordkeeping requirements	Included	Excluded
6	Secure Area	Defined	Clarified in preamble and revised requirements for facilities to allow facilities to submit amendment to security plans to change access control/secure area
7	Lost/Stolen/damaged cards	Access procedures defined in TWIC Addendum	Specific requirements included in regulation – employee will receive access to secure areas for up to 7 days after card is lost/stolen/damaged; TSA expects to have replacement card issued within 3-4 days.
8	Area Maritime Security Committee members (these people see SSI)	Need TWIC	Need name-based check to serve on Committee if member is not already required to hold a TWIC



Final Rule Differences from NPRM (continued)

	Topic	NPRM	Final Rule
9	Vessels in foreign waters	No special provisions	Amended secure area definition so that certain U.S. vessels not required to have secure areas when working beyond US waters
10	Emergency responders	Not specifically addressed	Not required to obtain a TWIC for emergency response
11	Disqualifying crimes	Same as used for Hazmat endorsement	Bomb threats permanently disqualifying (but eligible for waiver); welfare fraud and hot checks no longer considered crime of “dishonesty, fraud . . .”; new list applies to TWIC & HME
12	Card Readers and Biometric Authentication	Owners and operators biometrically authenticate individuals at access control points	Owners/operators not required to install biometric readers. CG will conduct random and scheduled spot checks of TWICs and will biometrically authenticate individuals during these checks.
13	Administrative Law Judge	Not included	May be used for waiver denials and appeals of disqualification based on intelligence. Applies to TWIC, Hazardous Materials Endorsement (HME), and air cargo applicants

