



# MARITIME EXCHANGE

for the Delaware River and Bay

## TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) FACTS

### ◆ TWIC RULEMAKING STATUS

- In response to comments received on the joint TSA/CG Notice of Proposed Rule Making (NPRM) published 22 May 2006, TSA and Coast Guard 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 second rulemaking. The public will have opportunity to comment on the technology and access procedures which will be proposed 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.
- All USCG credentialed merchant mariners.
- TSA estimates ~ 750,000 maritime workers will require TWICs.

### ◆ ENROLLMENT PROCESS

- Optional phone or web-based pre-enrollment (applicant provides basic information).
- Recommended, but not mandatory; will provide applicant with appointment time and reduce time at enrollment center.
- 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.
- TSA Conducts a Security Threat Assessment (STA).
- Upon successful completion of the STA the TWIC is produced 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 appeal and waiver rights.
- Applicant returns to enrollment center to claim credential for use at MTSA regulated vessels, facilities, and OCS facilities.

### ◆ TWIC FEES

Standard TWIC Enrollment	\$137.25
Hazmat/Mariner/FAST TWIC Enrollment	105.25
Lost/Damaged Card Replacement	36.00 (Note: may increase to \$60)

### ◆ DHS AGENCY RESPONSIBILITIES

- **TSA Responsibilities**
  - TWIC enrollment
  - Security threat assessment and adjudication
  - Card production
  - TWIC issuance
  - Appeal/waiver for TWIC denials



### TSA Responsibilities (cont.)

- 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

#### ♦ **SECURITY THREAT ASSESSMENT**

- Criminal History Records Check
  - Fingerprint and Name / Biographic-Based
  - Permanent Disqualifying Offenses
  - Interim Disqualifying Offenses
  - Wants/warrants and indictments
- Immigration 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 federal crime of terrorism or comparable State law
  - 5) A crime involving a Transportation Security Incident (TSI) Note: A TSI is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. The term "economic disruption" does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute
  - 6) Improper transportation of a hazardous material under 49 U.S.C. 5124 or a comparable state law
  - 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 where one of the predicate acts consists of one of the permanently disqualifying crimes
  - 11) Attempt to commit the crimes in items (a)(1)-(a)(4)
  - 12) Conspiracy or attempt to commit the crimes in items (a)(5)-(a)(10)



### Disqualifying Offenses (cont.)

- **B. Interim Disqualifying Criminal Offenses** -- Conviction within 7 years, or release from incarceration within 5 years of application
  - 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 (except welfare fraud and passing bad checks)
  - 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 kill
  - 12) Robbery
  - 13) Fraudulent entry into a seaport
  - 14) Lesser violations of the RICO (Racketeer Influenced and Corrupt Organizations) Act
  - 15) Conspiracy or attempt to commit crimes in this paragraph
  - 16) Indictments, wants/warrants for any disqualifying crime until released

### ◆ **SECURE AREAS**

- The area on board a vessel or at a facility or OCS facility over which the owner/operator has implemented security measures for access control.
- Does not include passenger access areas, employee access areas, or public access areas as defined in 33 CFR Parts 104.106, 107, and 105. 106 respectively.
- In other words, the secure area would be anything inside the outer-most access control point of a facility, and it would encompass the entirety of a vessel or OCS facility (Ref: Federal Register/Vol. 72, No 16 p.3498).

### ◆ **RESTRICTED AREAS**

- Restricted areas fall within the perimeter and are defined as areas that require limited access or higher degrees of security.
- Facility owners/operators have the discretion to designate their entire facility as a restricted area. In this situation, the restricted area and secure area would be one and the same.
- Option for facility owners/operators to redefine their secure area, to include only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident.
- Maritime Transportation Related Areas.
- Includes: Piers, tanks farms, storage areas (warehouses), container yards.

### ◆ **ACCESS CONTROL – NEW HIRE PROVISION**

- This provision is intended to limit the risk presented by an individual who has not undergone a full security threat assessment and has not been issued a TWIC, while balancing the need to enable individuals to begin work as soon as possible.



- Applies to direct employees of a facility; does NOT include longshoremen, truck drivers, contractors, vendors, and other visitors and may NOT be used to grant accompanied access to individuals being hired as Facility Security Officers (FSO).
- Allows newly-hired employees to work while waiting for issuance of their TWICs.
- Employer must apply for provision via HOMEPART after employee has completed TWIC enrollment; information must be entered exactly as given at enrollment center for HOMEPART to match to enrollment record. Items requested include:
  - Full legal name
  - Date of Birth
  - Social Security number
  - Employer name and 24 hour contact number
  - TWIC date of enrollment of enrollment
- 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; this may be extended for an additional 30 days by the cognizant COTP if TSA has not yet issued the new hire's TWIC.

#### ◆ **Provisions for Accompaniment of New Hires**

- All measures for access control and monitoring from the security plan must be followed.
- No more than 25% of a facility's employees may have access under this provision at one time.
- No more than 25% of employees in each work unit may be new hires.
- This provision is only available to new hires who are assigned to work units of no more than 25 employees.
- The new hire may be considered accompanied if provisions 1 & 2 are met and are in a work unit of no more than 25 people.

#### ◆ **TWIC AND ACCESS CONTROL**

- The facility owner or operator must ensure the implementation of security measures to prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.
- The facility owner or operator must ensure the means used to establish the identity of individuals not in possession of a TWIC, in accordance with 101.515 of this subchapter and the procedures for escorting them are specified.
- Personal Identification must meet the following requirements:
  - Be laminated or otherwise secure against tampering
  - Contain the individual's full name
  - Contain a photo that accurately depicts the individual's current facial appearance
  - Bear the name of the issuing authority
- The facility owner or operator must ensure that a TWIC program is implemented as follows:
  - All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access.
  - This inspection must include:
    - A match of the photo on the TWIC to the individual presenting the TWIC.
    - Verification that the TWIC has not expired.
    - A visual check of the card to determine whether the TWIC has been tampered with or forged.
- If an individual cannot present a TWIC because it has been lost, damaged, or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a



### Access Control (cont.)

valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if:

- The individual has reported the TWIC as lost, damaged, or stolen to TSA.
- The individual can present another acceptable identification credential.
- There are no other suspicious circumstances associated with the individual's claim of loss or theft.
- If an individual cannot present his or her TWIC for any other reason he or she may not be granted unescorted access to the secure area. The individual must be under escort at all times while inside of a secure area.
- 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 is granted.
- This may be accomplished by having a side by side companion or monitoring.
- Monitoring must enable sufficient observation of the individual to determine if they are engaging in unauthorized activities or in an unauthorized area.
- Monitoring may be accomplished by:
  - Use of a closed circuit television system that is monitored by a TWIC holder.
  - A combination of roving security patrols, automatic intrusion devices or surveillance equipment.
  - An individual without a TWIC may not enter restricted areas without having an individual who holds a TWIC as a side by side companion.

### ♦ **ENFORCEMENT FOR THE IMPLEMENTATION OF TWIC**

- **TWIC Verification by Vessel/Facility Personnel:**
  - Identifying Deficiencies
    - > Check TWIC for signs of tampering and authenticity.
    - > Visually compare the TWIC to the individual.
    - > Question the individual (remember, security personnel have the authority to do so).
  - Steps to take for verification of a TWIC
    - > Attempt to check person's identity by using an alternate form of identification.
    - > ASK the individual to remain at the access control point.
    - > Notify the Coast Guard Situational Unit Controller (215-271-4807) and await further instruction.
    - > Prevent unescorted access at minimum.
  - What NOT to do
    - > DO NOT attempt to restrain the individual or inform him he may not leave.
    - > DO NOT attempt to confiscate the TWIC from the individual.
  - Suspicious Activity
    - > Multiple TWIC cards suspected to be fraudulent presented for access in a short period of time.
    - > Attempting to access multiple times with same suspected fraudulent TWIC.
- **TWIC Verification by the Coast Guard:**
  - Visual Inspection.
  - Handheld readers to verify TWIC information. Will match biometric template on the TWIC with fingerprint of the individual presenting the TWIC and will provide PIN number.
  - Occurs during MTSA spot checks, annual exams, and random TWIC spot checks or when notified of a fraudulent or invalid TWIC from the facility.



- **Coast Guard Enforcement on the Facility:**

- Types of enforcements include:
  - > On-the-spot corrections
  - > Deficiency reports
  - > Letter of Warning
  - > Notice of Violation
  - > Civil Penalties

- **Coast Guard Contacts**

- All suspicious activity must be reported to the National Response Center (NRC) at 1-800-424-8802
- Report a single fraudulent or invalid TWIC to the COTP by notifying the Situation Unit Controller at 215-271-4807

- ◆ **FUTURE MILESTONES – DEPLOYMENT & COMPLIANCE**

- Enrollment will begin no sooner than 26 March 2007.
- 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 to be 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.

- ◆ **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 within 15 months after effective date of the final rule.
- Work with various federal organizations and private industry to finalize specifications for a contactless biometric TWIC reader.
- Coast Guard published a notice of availability for the NMSAC recommendations contactless biometric software specification for TWIC cards.
- TSA published a notice announcing the fee amounts.
- Conduct pilot test of TWIC contactless biometric readers and credential validation processes.