



MARITIME EXCHANGE

for the Delaware River and Bay

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

Program Update as of February 7, 2007

Contact: Lisa Himber
Maritime Exchange for the Delaware River and Bay
215/925-2615
lisa.himber@maritimedelriv.com
Documents at: www.maritimedelriv.com/Port_Security/TSA/TSA_Port_Security.htm

Key Dates

- The rule is effective March 26, 2007.
 - Comments on Card Replacement Fee must be submitted by February 26, 2007.
 - On January 29, TSA awarded a \$70 million TWIC contract to Lockheed Martin.
 - Compliance dates for individual regions will be rolled out by COTP zones. Notice for these deadlines will be published in the Federal Register providing 90 days advanced notice prior to required use. The SAFE Port Act requires that the TWIC be deployed in the top 10 ports on the basis of risk by July 1, 2007. Full compliance for all ports and mariners is September 25, 2008.
 - **The Port of Wilmington has been targeted as the first port in the U.S. for TWIC deployment.**
 - Voluntary compliance will begin on or about March 26.
 - Mandatory compliance will begin 90 days after publication of the date in the *Federal Register*, anticipated sometime in February.
 - The following are listed as possible Delaware River enrollment center locations, but TSA and Coast Guard will work with the community to revise the list as necessary.
 - Philadelphia, Chester, Marcus Hook and Penn Manor, PA
 - Camden and Paulsboro, NJ
 - Wilmington and New Castle, DE
 - At this point, it is expected that full compliance for all of sector Delaware Bay will be required by the end of September, 2007.
-

Key Provisions

Reference the TWIC final rule published 1/25/07 and the draft Coast Guard Draft Navigation and Vessel Inspection Circular (NVIC). Both are published on the Maritime Exchange web site as above.

- The regulation addresses the application, issuance, and initial use of the TWIC as a means of personal identification when seeking access to secure areas of regulated vessels and facilities. It does not contain provisions for TWIC biometric readers that would require the verification of biometric data stored within the TWIC with the individual presenting the TWIC for access.
 - TWIC enrollment will be conducted by TSA's Trusted Agent.
 - TSA will use a combination of fixed and mobile enrollment centers.
 - Employers will be required to inform employees of the need to obtain a TWIC and how they can apply for one.
 - Owners/operators must give individuals at least 60 days notice to begin the enrollment process.



Key TWIC Provisions (cont).

- TSA estimates that it will take between 10 and 30 days to do the security threat assessment.
- Applicants must provide certain identity documents, submit fingerprints, be photographed, and sign application documents at the time of enrollment.
- Applicants will also be required to pay the fee in cashier's check, money order or credit card.
- TSA will notify the applicant when the credential is ready for pick-up and what processes are necessary to activate the TWIC.
- *For more detail, see NVIC at pages 12-20.*
- Fees for a TWIC are proposed to range from \$107 to \$159 depending on whether or not the individual has previously undergone a security threat assessment. TSA is seeking comments on these fees. A subsequent press release announced the cards would cost \$137.25.
- Provision for new hires that permits accompanied access for such individuals in the period between application and receipt of the TWIC. The rule is silent on how to address casual labor.
 - Once an individual has applied for a TWIC and has undergone the name-based security check he can be granted access to a secure area, as long as he is accompanied by an employee who has a TWIC, for up to 30 days, and perhaps longer, with Coast Guard approval.
 - This provision cannot be used to allow temporary unescorted access to contractors, vendors, longshoremen, truck drivers (unless they are direct employees of the owner/operator), any other visitor, or if the new hire is a Company, Vessel, or Facility Security Officer, or is otherwise tasked with security duties as a primary assignment.
 - *For more detail see NVIC at pages 32-34.*
- Individuals must report lost or stolen (or forgotten for the day) cards to the TWIC Call Center. Absent suspicious circumstances, such individuals may have unescorted access for a period of up to 7 days within a calendar year.
 - *For more detail see NVIC at page 35.*

Permanent Disqualifying Acts

- Treason, sedition, espionage, and terrorism as well as conspiracy to commit these acts
- Crime involving a transportation security incident
- Improper transportation of hazardous materials
- Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device
- Murder
- Making any threat, or maliciously conveying false information, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, state or government facility, public transportation system, or an infrastructure facility
- RICO violations where the predicate is one of the crimes listed
- Conspiracy or attempt to commit these crimes

Interim Disqualifying Offenses – Convicted of the following within past seven years or released from incarceration within five years of TWIC application.

- Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon.
- Extortion



Interim Disqualifying Offenses (cont).

- Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering (welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation)
- Bribery
- Smuggling
- Immigration violations
- Distribution of, possession with intent to distribute, or importation of a controlled substance
- Arson
- Kidnapping or hostage taking
- Rape or aggravated sexual abuse
- Assault with intent to kill
- Robbery
- Conspiracy or attempt to commit the crimes listed
- RICO violations for fraudulent entry into secure seaport area

Definition of Secure Area

The draft NVIC clarifies how the TWIC program will be implemented. Of significance includes the clarification of the difference between restricted and secure areas. In its simplest form, a secure area is everything inside the perimeter of a facility or vessel; restricted locations are sites within secure areas where additional security measures may be required.

- Any TWIC holder can serve as an escort to a non-TWIC holder.
- In a secure area, one TWIC holder can escort up to 10 non-TWIC holders, and that escort does not mandate physical, side-by-side but can include random patrols or monitoring via video (for example, a contractor coming in to fix an antenna may not require constant side by side escort).
- In a restricted area, the ratio of escort is 1 to 5, and constant physical escort is required.

It is important to note that the regulation sets the minimum requirements. Individual owners/operators will determine access control and escort requirements for their vessels and facilities.

The TWIC rulemaking allows (but does not require) facilities to amend their security plans to revise their restricted/secure areas. The idea is to allow facilities to reconfigure fences, etc., so that non-maritime locations (such as administration buildings or manufacturing locations) can remain outside the regulated areas. These amendments are due six months after the publication of the Final Rule.

TWIC Privacy Policy

TSA recently released a copy of the December 29, 2006 TWIC Privacy Policy Assessment. In addition to reiterating what data is to be collected, how it will be used, and some of the procedures for protecting data during TWIC application, waiver and adjudication processes, the document also outlines:

- How long personal information will be retained
- Agencies within DHS and externally with which the data may be shared
- How information is to be shared
- Contractor and Information Technology personnel access to data



NMSAC TWIC Working Group/Phase II Deployment

The National Maritime Security Advisory Committee TWIC Working Group has been tasked to develop specifications which will be used in Phase II of the TWIC deployment. The SAFE Port Act requires that TSA start a pilot program to test the card readers by April 1.

The issue is that the current national standard will not allow for the transfer of biometric data (fingerprint) from the card to the reader in a contactless (that is, without swiping a card in a reader) mode. The working group is also developing a set of recommendations on how to implement the pilot program at maritime facilities and vessels.

Exchange VP Lisa Hember is co-chairing this work group, which is charged to complete its task by February 28. At that time, TSA will distribute the reader specification for public comment.

In January, the group completed a set of maritime operating requirements (e.g., response time once the card and biometric have been presented to the reader must be less than three seconds). From this document, the technology industry representatives on the work group will draft a reader specification.

TSA indicates they are still on track for an April 1 pilot program start. In a sense, they have already started a pilot program by identifying pilot locations and starting to develop processes. (Currently, TSA and the Ports of Los Angeles and Long Beach have signed agreements for the pilot program.) The reality is that once a specification is developed, at least six to nine months will be required to build, certify and test the new readers.

The plan is for pilot program participants to apply for Port Security Grant funding to purchase the test readers. At this point, TSA does not plan to award a federal contract to a single provider for the pilot program but expects that each participating vessel and facility will contract with its own vendor.

Moving Forward

At this point, the regulation has been finalized and there are no further opportunities for maritime stakeholders to provide comment to the TSA.

TSA does plan to create a stakeholder Advisory Board to assist in the TWIC deployment.

We can and will work with local Coast Guard once the NVIC is finalized and afterwards to develop procedures to implement the program in this region. The Coast Guard is coordinating a TWIC Workshop for Facility Security Officers on March 7. Other outreach meetings will be scheduled over the next several weeks.

Coast Guard and TSA Headquarters personnel are working to draft a separate rulemaking which will govern the deployment of the TWIC readers and establishment of electronic communications between vessels/facilities and the TSA database. Coast Guard will publish a proposed rule, perhaps by the summer, which will include a public comment period.

TWIC stakeholders are encouraged to contact the Exchange with any questions, suggestions, or concerns about the program.





Summary of Significant Changes Proposed and Final Rule

Topic	NPRM	Final Rule
Access control	Visual identity badge and reader (with biometric verification and validity check at facility/vessel based on MARSEC level)	Visual identity badge; Coast Guard conducts periodic checks of biometric and validity (second rule for reader requirements)
Escorted access	Definition only	Definition modified to clarify that in restricted areas (33 CFR 101.105), "escort" means a side-by-side escort; outside restricted areas, "escort" may consist of monitoring
New hires	Not granted unescorted access to secure areas until successful completion of security threat assessment and card issuance	Permitted to have limited access for 30 consecutive days if accompanied by TWIC-holder and additional requirements are met
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)
TWIC Addendum and recordkeeping requirements	Included	Excluded
Secure area	Definition only	Clarified definition's meaning in preamble, and revised part 105 to allow part 105 facilities to submit FSP amendment to change access control area
Lost/Stolen/Damaged cards	Access procedures defined in TWIC Addendum	Specific requirements included in regulation
AMS Committee members	Need TWIC	Need name-based check or a TWIC
Vessels in foreign waters	No special provisions	Changed secure area definition to state that at certain specified times, U.S. vessels may not have any secure areas
Emergency responders	Not specifically addressed	Not required to obtain a TWIC for emergency response
Voluntary compliance	Offered	Not offered
Compliance dates	12-18 months after final rule	Phased for facilities by each COTP zone. All mariners and vessels 18 months after effective date of final rule
Disqualifying crimes	Same as those used for HME	Amended; new list will apply for both TWIC and HME
Administrative law judge (ALJ) review	Not included	May be used for waiver denials and disqualifications under § 1572.107
Immigration standards	Limited ability for non-U.S. citizens to obtain TWICs	Expanded to cover foreign maritime students, and certain professionals and specialists on restricted visas; permitting aliens in TPS to apply for a waiver
Mental incapacity	Could only be waived by showing court order or letter from institution	Waiver broadened to allow for "case-by-case" determinations
Fee	\$95 - \$149; card replacement fee \$36	\$107-\$159; card replacement fee \$36, but requesting comment on increasing this fee to \$60