



Transportation
Security
Administration

Public Affairs Guidance

Port Security/TWIC Program- Final Rule

LAST MODIFIED

1/3/2006 9:00 A.m.

GUIDANCE

- Media calls on TWIC should be referred to DHS Public Affairs at (202) 282-8010
- Media calls on the Merchant Mariner Credential should be referred to Coast Guard Public Affairs at (202) 372-4633
- DHS OPA will farm out calls as needed.

PRODUCTS

- Background
- Talking Points
- Q&As

BACKGROUND

In accordance with the requirements of the Maritime Transportation Security Act (MTSA) and the SAFE Port Act, the Transportation Worker Identification Credential (TWIC) will serve as an identification card for all personnel requiring unescorted access to secure areas of Maritime Transportation Security Act (MTSA) regulated facilities and vessels and all mariners holding Coast Guard issued credentials or qualification documents. To obtain a TWIC, an individual must successfully pass a security threat assessment conducted by the Transportation Security Administration (TSA). A structured waiver and appeals process will be in place for unfavorable threat assessment results, as required by MTSA.

TALKING POINTS

- TWIC will serve as a common credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners holding Coast Guard-issued credentials. The TWIC program will issue workers a tamper-resistant "Smart Card" containing the worker's biometric (fingerprint template).
- Controlling access to secure areas is a critical component of DHS' efforts to enhance port security.
- Regulations in the final rule reflect input obtained through four public meetings and over 1,900 comments to the federal register.
- TSA, in partnership with the U.S. Immigration and Customs Enforcement and the Federal Bureau of Investigation, will conduct threat assessments on individuals who require TWICs. The Coast Guard will work with the owners and operators of vessels, port facilities, and Outer Continental Shelf (OCS) facilities to implement TWIC access control requirements.
- The Maritime Transportation Security Act of 2002 changed the landscape of port security by setting out specific requirements for owners and operators of certain vessels and port facilities. These owners and

operators were required to conduct security assessments, create security plans specific to their needs and submit the plans to the Coast Guard. The Coast Guard approves and monitors compliance with these plans.

- TSA and the Coast Guard are working to implement TWIC in the maritime mode beginning in March 2007. Other transportation modes will be considered for TWIC in the future. The implementation will comply with the schedule established in the SAFE Port Act in order of port priority as published in DHS' Infrastructure Protection Program.
- An estimated 750,000 workers will require TWICs and up to 850,000 credentials may be produced over an 18 month period to address turnover and replacement cards.
- Owners and operators are not required to purchase, install, or maintain card readers until technologic and logistic improvements are complete. Until card readers are in place, workers requiring unescorted access to secure areas will present their TWIC to authorized personnel for entry. The Coast Guard will conduct unannounced checks using handheld readers to confirm the identity of TWIC holders and the validity of the credential.
- A second rulemaking, expected calendar year 2007, will propose the requirement for biometric readers and will further propose access control requirements. The second rulemaking will provide an opportunity for additional public comment.
- The security threat assessment includes: (1) a check against terrorist watch lists; (2) an immigration status check; and (3) a FBI fingerprint-based criminal history records check. This TSA-performed security threat assessment is the same as for those applying for, transferring or renewing a hazmat endorsement on their state-issued commercial drivers licenses (CDLs).
- TWIC holders will be eligible for unescorted access to secure areas of the nation's: 3,100 MTSA regulated port facilities; 10,000 vessels; and 62 Outer Continental Shelf (OCS) facilities. Owners and operators will determine which areas of their vessel or facility are deemed as secure areas and who is ultimately granted access. The Coast Guard will distribute a Navigation and Vessel Inspection Circular (NVIC) to provide additional guidance on requirements for the TWIC Program.
- Applicants who are denied a TWIC will be provided with information on why they were denied and instructions on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes or aliens in Temporary Protected Status. Applicants who are aware of a potential disqualifying crime may apply for a waiver when first applying for a TWIC to expedite the waiver process. Applicants who seek a waiver and are denied may seek review by an Administrative Law Judge (ALJ).
- Over the past six months, TSA completed name-based threat assessments on port workers and longshoremen. The assessments included a legal work status check and checks against terrorist watch lists. This was an interim measure to immediately raise the bar on security at port facilities.

Key Measures

TSA and the Coast Guard held four public meetings, reviewed over 1,900 comments from stakeholders, listened to comments from the Small Business Administration and Government Accountability Office. The following requirements are included in the final rule:

- **Ineligibility** - An individual who lacks lawful presence and certain immigration status in the United States, has a connection to terrorist activity, or was convicted of the following crimes will be ineligible for a TWIC. *Crimes listed in Q&A.*
- **Cost** - **As proposed in the Final Rule, the fee for a TWIC card will be between \$139 and \$159, for cards that are good for 5 years. TSA proposes that workers with current, comparable background checks (HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade (FAST)) will receive a discounted fee between \$107 and \$127. The exact amount of the fee will be finalized once a contract is awarded in early 2007. A subsequent Federal Register Notice will be issued at that time.**
- **Privacy and information security** - These components are critical to the TWIC program. "Trusted Agents" who undergo a TSA security threat assessment will collect biometric and biographic enrollment data. This information is deleted from the enrollment center work stations once the applicant completes enrollment. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which encrypts all personally identifying information at very high standards before it is transferred or stored, and

- protects the data from unauthorized use.
- Use - During the initial rollout of TWIC, workers will present their cards to authorized personnel, who will compare the holder to his or her photo, inspect security features on the TWIC and evaluate the card for signs of tampering. The Coast Guard will verify TWICs when conducting vessel and facility inspections and through spot checks using hand-held readers, ensure credentials are valid. Until card reader technology is tested and a regulation issued on access control, facility owners and operators will not be required to utilize card readers.
- Population - An estimated 750,000 individuals will be required to obtain a TWIC. This includes **port facility employees, longshoremen, truck drivers, mariners and others requiring unescorted access to secure areas of maritime facilities and vessels.**
- Biometric data - Applicants will provide a complete set of fingerprints and sit for a digital photograph. Fingerprints will be used for the security threat assessment and to create the template for the biometric information stored on the credential.
- Required documentation - Applicants must provide the appropriate documents in order to verify their identity. Some of these include a U.S. passport, drivers' license, or U.S. Certificate of Naturalization. The complete listing of required documents will be available on the TWIC website at www.tsa.gov/twic.
- Technology - **The credential will be a Smart card containing the applicant's photograph and name, an expiration date, and a serial number. In addition, an integrated circuit chip will store the holder's fingerprint template, a PIN chosen by the individual, and a card holder unique identifier.**
- Enrollment process - Applicants are encouraged, but not required, to "pre-enroll" at the TWIC web site. The convenience of pre-enrollment reduces waiting time at the enrollment centers. Although applicants may schedule an appointment to complete enrollment at an enrollment center, appointments are not required. At the enrollment center, pre-enrolled applicants must provide documents to verify their identity, confirm the accuracy of pre-enrollment information, provide biometric information (a full set of fingerprints and a facial photograph), and sign the enrollment documents. Applicants who did not pre-enroll will also need to provide biographic information. All applicants will receive a privacy notice and consent form, by which they agree to provide personal information for the security threat assessment and credential. The enrollment process for a pre-enrolled applicant is expected to take approximately 10 minutes. The enrollment process for an individual who chose not to pre-enroll is expected to take approximately 15 minutes.
- Security threat assessment - The assessment includes a criminal history records, a check against terrorist watch lists and an immigration status. If no adverse information is disclosed, TSA typically completes a security threat assessment in less than 10 days. However, processing time increases for an applicant with a criminal history or other disqualifying information, and is further lengthened if the applicant initiates an appeal or waiver.
- New Direct Hires: TSA and the Coast Guard have added a provision in the TWIC Final Rule to allow owners and operators to give new directly hired employees limited access to secure areas while their applications for a TWIC and security threat assessments are being processed. The newly hired employees must have completed a name-based terrorism check and the owners and operators must comply with additional requirements. By using the provision, the new employees may begin working without undue delay.
- TWIC issuance -- The applicant will be notified by email or phone, as indicated on their application, when his/her credential is available at the enrollment center. The applicant must return to the same enrollment center to pick up his/her TWIC. The TWIC will expire five years from the issue date.
- TWIC help desk - When the enrollment contract is awarded, a toll-free TWIC help desk will provide service for merchant mariners, transportation workers, facility and vessel owners and operators, and others who require assistance related to the TWIC program. Assistance includes help for pre-enrollment; enrollment; and, lost, stolen, or damaged card reporting and credential replacement.
- Rollout Schedule - The TWIC rollout plan will be posted to the TWIC web site at www.tsa.gov/twic. The deployment schedule will comply with the requirements in the SAFE Port Act in order of port priority as published in DHS' Infrastructure Protection Program. Enrollment and compliance dates will be phased in by Captain of the Port (COTP) zone. Enrollment for the existing workforce should be completed within 18 months

QUESTIONS and ANSWERS

Q. Is DHS concerned that the TWIC implementation will result in a significant negative impact on commerce because many workers may be disqualified because of criminal history or immigration status?

A. The TWIC program is designed to enhance security and facilitate commerce. As the program is rolled out, TSA and the Coast Guard are working closely with port facilities to address concerns that arise. TSA has a robust appeal and waiver process to mitigate adverse impacts on the industry for workers with prior criminal activity.

Q. Has a contractor been selected for the TWIC program? Will the American Association of Airport Executives (AAAE) still play a role in TWIC?

A. TSA and Coast Guard received final proposals from contractors interested in deploying the TWIC program and the current plan is to award a contract in January 2007. AAAE was not among the eight companies selected as qualified vendors.

Q: How much have you spent so far on TWIC? What have you gotten for the money?

A: Since 2002, approximately \$94.7 million has been spent on the TWIC program. This investment funded the development of information technology and equipment, evaluation of data storage alternatives, and strategic and project planning support to start up the program. TSA conducted prototype testing at 26 sites in six states in 2005.

Q: How much will port workers be charged for a TWIC?

A: The fee for TWIC is between \$139 and \$159 and the card is good for 5 years. The contract for enrollment and operation of TWIC will be awarded soon. A subsequent Federal Register Notice will be issued at that time to notify stakeholders of the exact fee amount. Once the contract is awarded the final fee will be set. Workers with current, comparable background checks (HAZMAT, merchant mariner documents (MMD) or Free and Secure Trade (FAST) will receive a discounted fee between \$107 and \$127.

Q. What measures are in place to protect small businesses, such as small passenger vessels?

A. TSA and the Coast Guard worked very closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers who do not require unescorted access to secure areas such as the pilot house and engine room. Employee access areas are those areas which support the passenger areas and crewmembers who would likely be in these areas would be waiters, entertainers, and galley staff. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas.

The production and distribution of a Small Business Compliance Guide, special access benefits for newly hired employees, an informational web site and a live help desk are under development to assist small businesses successfully implement the program.

Small business input will also be crucial in the development of card reader technology so that TSA and the Coast Guard can implement TWIC in a way that meets the needs of all stakeholders.

Q. Why did TWIC take so long to get to this point?

A. TWIC is one component of the comprehensive port security enhancements put into place by the U.S. Coast Guard and TSA. TWIC implementation has presented unique challenges, which have been compounded by a rapidly changing technology landscape and the added demands of operating in the maritime environment.

During the past three years, TSA developed technology and tested the processes to collect and protect personal data, conduct security threat assessments, issue credentials and provide for sustained screening operations. In May 2006, TSA and the Coast Guard began the rulemaking process by laying out the government's proposal for how the program would be administered. Despite the fact that over 1,900 comments were received and the process traditionally takes over a year, the final rule was issued well in advance of the normal time required. Once the rule is published, TSA and the Coast Guard will move quickly to rollout the program and enhance port security.

Q. What technologies are being used in the national rollout?

A: The TWIC will be a Smart Card (i.e., a card with a small integrated circuit chip embedded in the card) and will contain the following technologies:

- Dual Interface Integrated Circuit Chips (ICC) - a small computer chip that can be read by either inserting the card in a slot in a "contact" card reader; or, holding the card within 10 centimeters of a "contactless" card reader
- Magnetic Strip - commonly found on the back of credit cards; read by "swiping" the card through a magnetic stripe card reader
- Linear Bar Code - commonly used to quickly identify items by scanning the codes with an optical reader—i.e. scanning grocery items at a checkout counter

Process

Q. Will you rollout TWIC to all ports immediately? How long before this card is in use for access control nationwide?

A. No, the initial enrollment will be phased, based on criticality. While we cannot provide an exact list of those ports for security reasons, we can say that these calculations are based on the size, volume, location, type of materials imported/exported and the number of employees at the port. We anticipate it will take 18 months to vet and issue credentials to the estimated 750,000 workers who will be required to obtain a TWIC.

Facilities will be required to use the TWIC as an access control measure on different dates according to COTP zone. These dates will be published in the Federal Register as enrollment progresses. We will also support local outreach to industry and worker groups to ensure all concerned are aware of enrollment schedules and requirements. Vessels and merchant mariners will be required to use TWIC as an access control measure 20 months after the publishing date of the final rule.

Q. What is required from a worker to apply for a TWIC?

A. During the enrollment process **applicants will visit an approved enrollment site operated by a TSA trusted agent, where they will provide proof of identity, biographic information (such as date of birth, address, phone number, physical characteristics, etc.), and be photographed and fingerprinted. The location of enrollment sites will be announced shortly.**

Q. Will a machine read these credentials? Who will pay for the equipment?

A. Facility and vessel owners are not required to purchase, install or utilize card readers at this time. A subsequent rulemaking will address card reader requirements.

Eligibility

Q. How will workers' information be collected when applying for a TWIC?

A. Trusted agents - employees of a vendor under contract to TSA - will collect all information (biometric and biographic) required at enrollment centers located throughout the country. TSA will store the information.

Q. What are the disqualifying crimes?

A. While a comprehensive list of crimes can be found on TSA's web site, the following covers all categories of offenses which permanently bar an individual from receiving a TWIC. Permanent disqualifying criminal offenses include: espionage, sedition, treason, terrorism, improper transportation of a hazardous material, unlawful possession, use, or sale of an explosive, murder, threats to a place of public use (government facility, public transportation system, or infrastructure facility), violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act in which the predicate act is one of the permanently disqualifying crimes, a crime involving a transportation security incident.

A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. A work stoppage, or other nonviolent employee-related action, resulting from an employer-employee dispute is not a transportation security incident.

Individuals are ineligible if convicted in the last seven years or incarcerated within the last five years of the following crimes: Unlawful possession, use or sale of a firearm or other weapon, extortion, fraud, bribery, smuggling, immigration violations, distribution or importation of a controlled substance, arson, kidnapping or hostage taking, rape or aggravated sexual abuse, assault with intent to kill, robbery, RICO violations that do not involve a permanent disqualifying crime.

Convictions for espionage, sedition, treason and terrorism are not eligible for a waiver.

Q: Is there going to be an appeal process for the security threat assessment?

A. Applicants who are denied a TWIC will be notified of the reason for denial and instructed on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification, and may apply to TSA for a waiver if disqualified for certain crimes, or if they are aliens in Temporary Protected Status. Applicants who are aware of a potential disqualifying crime may apply for a waiver when first applying for a TWIC to expedite the waiver process. Applicants who seek a waiver and are denied may seek review by an Administrative Law Judge (ALJ).

Q. Will a non-U.S. citizen be able to get a TWIC?

A. Yes. The rule includes a list of various immigration categories that are eligible to apply for a TWIC, including nationals, refugees, asylees, lawful non-immigrants with unrestricted work authorization, and certain professionals with restricted work authorization.

Q. During the prototype phase TSA tested the card in other modes of transportation. Will this credential be required for rail or airport employees?

A: The initial rollout of TWIC will be focused on the maritime mode, which will include rail workers and truck drivers who require unescorted access to secure areas of MTSA-regulated facilities, and vessel personnel. Once the initial maritime rollout is complete DHS will look at the possibility of requiring use of the credential in other modes of transportation.

Access Control

Q. By excluding access control from the final rules isn't this yet another delay in a program

that is already long past its intended implementation date?

A. The single greatest security benefit of TWIC is the ability to screen out port workers who pose a security threat. The final rule allows the federal government to begin that process in early 2007. The rule does include access control requirements, since TWICs will be required for any worker requiring unescorted access to secure areas of vessels and facilities. A second regulation will propose card reader requirements that utilize all of the unique technologies employed in the TWIC.

Card reader requirements were delayed in response to concerns by port operators and workers about the processes and emerging technologies involved in access control. As we move forward with security threat assessments and card issuance, we will work with those affected to ensure card readers and access control systems enhance security while minimizing the impact on maritime transportation and commerce.

Q. The GAO stated that TSA needed to conduct more testing before implementing the TWIC program. Why is TSA moving forward with the rule?

A. Testing advanced reader technology is critical to the program's success, and will take place concurrently with the steps we are taking now to enhance port and vessel security. The current rule allows us to begin collecting biometrics and conduct an in-depth security threat assessment of all individuals who require unescorted access to secure areas of MTSA regulated vessels and facilities. We will continue to work closely with facility and vessel owners and operators, port authorities, workers, and private industry to address card reader issues. Once reader testing is completed, that function will be added to the TWIC program to further enhance port security.

DHS is already working with the port authorities of Los Angeles and Long Beach to test access control technologies and equipment in the marine environment, in accordance with the SAFE Port Act. Other locations will also be identified for additional testing. The Coast Guard and TSA have, with industry participation, initiated the development of contactless reader technology. In addition, the National Maritime Security Advisory Committee (NMSAC), representing maritime industry leaders, is taking an active role in recommending technical and operational requirements for a contactless TWIC card.

Q. How will ports control access to critical areas without card readers?

A. In addition to the current access control measures that vessels and facilities have identified in their security plans, TWICs will be required for entry and used as a visual identification badge. Workers will present their cards to authorized personnel, who will compare the holder to his or her photo, inspect security features on the TWIC and evaluate the card for signs of tampering. The Coast Guard will verify TWICs when conducting vessel and facility inspections and conducting random spot checks using hand-held readers to ensure credentials are valid and ensure the card holder is the rightful owner.

Name-Based Checks

Q: Who was screened during the interim screening and who will be required to obtain a TWIC?

A: Initial name-based security threat assessments were focused on port facility employees and longshoremen employed by regulated port facilities. With publication of the final rule, all workers who need unescorted access to secure areas must obtain a TWIC, including truck drivers, railroad workers, and vendors. Individuals who have already completed a comparable threat assessment (such as a merchant mariner's document, FAST cards or hazmat endorsement) do not need to undergo a second security threat assessment. However, these individuals must enroll in TWIC and provide the biometric and biographic information needed to issue the credential.

Q: Why were truck drivers and others excluded from the initial name-based screening?

A: Name-based background checks are an immediate security measure designed to limit individuals that pose a threat from gaining access to port facilities. This is a first step and will cover a large population of workers.

Merchant Mariner Questions

Q. Will these rules affect all Merchant Mariners?

A. Yes. Under law, all credentialed U.S. Merchant Mariners (this includes all persons holding a Coast Guard-issued merchant mariner's license, merchant mariner's document, or certificate of registry (COR)) must obtain a TWIC. With the implementation of TWIC, the Coast Guard merchant mariner document will no longer serve as an identification document, and will only serve as proof of the bearer's professional qualifications. The Coast Guard has drafted a proposed rule that would combine the elements of four merchant mariner professional credentials into one certificate called the Merchant Mariner Credential (MMC). The MMC would serve as the mariner's qualification credential, while the TWIC would serve as the mariner's identification credential. The Coast Guard and TSA are streamlining the process for the two credentials to reduce costs, duplications of effort and processing time for mariners. The Coast Guard will begin the issuance of the MMC 18 months after the effective date of the TWIC rulemaking and replacement will continue over a 5 year period at renewal of mariner documentation.

Q. How much will the MMC cost?

A. The cost of the MMC will be the same as the cost of the current mariner documentation. The only change will be the removal of additional issuance fees (\$45) as there will no longer be multiple credentials to issue.

Q. What are the overall costs of the MMC?

A. We foresee the MMC adding no additional cost to mariners, and in fact, it should reduce the overall cost burden. Merchant Mariners will submit information required for the MMC at TWIC enrollment centers when they apply for their TWICs. Mariners will only need to visit one of the 17 Regional Exam Centers when they need to take an examination as the MMC can be mailed after the visit to the TWIC enrollment center.

Prototype Questions

Q. How many transportation workers participated in the prototype evaluation?

A. As of December 31, 2005, more than 4,000 workers were issued Prototype TWICs. Participants in the Philadelphia and Los Angeles/Long Beach areas received TWICs after completing TSA-performed name-based threat assessment. Participants in the state of Florida underwent a criminal background check conducted by the state of Florida as well as the name-based assessment performed by TSA before being issued TWICs.

Q. Where did the prototype take place?

A. The prototype was conducted at 26 locations in the geographical areas of Los Angeles/Long Beach, Wilmington/Philadelphia and Florida's deepwater ports. Participation was voluntary for the prototype. Examples of participants included truck drivers, longshoremen, and container terminal and airport personnel.