TWIC Website FAQs

1. **What is a TWIC?**
   TWIC stands for Transportation Worker Identification Credential. As currently proposed, TWIC is a secure identification credential, that uses 'smart card' technology and is about the size of a credit card. Transportation workers would use TWIC to access secure areas of transportation facilities. The credential verifies the holder's worker's identity by linking that person's claimed identity and background information to the holder's biometric stored on the credential.

2. **Why is TSA proposing to require the use of TWIC at maritime facilities and vessels?**

   The Maritime Transportation Security Act (MTSA) requires use of a biometric ID credential and a security threat assessment for individuals who have access to secure areas of maritime facilities and vessels without an escort

3. **What are the benefits of the proposed TWIC program?**
   - Creates a tamperproof ID credential that may be used and accepted across all modes of the transportation system.
   - Creates a uniform, national standard for secure identification of transportation workers.
   - Reduces redundant credentials and background checks.
   - Provides a solution to positively and securely link an individual to a credential via biometrics and to the background information of that individual.
   - Ensures compatibility with existing facility access control systems to leverage current security investments.
   - Provides ability to revoke access privileges to TWIC holders who are identified as a threat
   - Is consistent with principles of Homeland Security Presidential Directive 12 (HSPD 12) and the Federal Information Processing Standards (FIPS) 201. FIPS 201 raises the Federal Standard for identity management business practices throughout the Federal Government, making the TWIC a trusted and universal ID card.

4. **What is the current status of the TWIC program?**

   The TWIC program has completed the Prototype Phase, in which a variety of technologies and processes were tested. TSA is now preparing for a full, nationwide implementation. TSA intends to competitively award a contract for system operation and maintenance, enrollment and help desk/call center for the TWIC program. The program will be governed by the regulations TSA and the United States Coast Guard issue. TSA and Coast Guard published a notice of proposed rulemaking (NPRM) on May 22, 2006 and that is available for review in the docket: http://dms.dot.gov or in the Federal Register, volume 71, page 29396. The public may comment on the NPRM until July 6, 2006. In addition, TSA and the Coast Guard will hold four public meetings to solicit public input. The four public meetings are currently scheduled as follows: Wednesday, May 31, 2006 in Newark, NJ; Thursday, June 1 in Tampa, FL; Tuesday, June 6 in St. Louis, MO; and Wednesday, June 7 in Long Beach, CA.

   You may submit comments identified by TSA docket number TSA-2006-24191 or Coast Guard docket number USCG-2006-24196 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:
   (1) Web site: http://dms.dot.gov.
   (2) Mail: Docket Management Facility, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street SW, Washington, DC 20590-0001.
   (3) Fax: 202-493-2251.
   (4) Delivery: Room PL-401 on the Plaza level of the Nassif Building, 400

Seventh Street SW, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.
(5) Federal eRulemaking Portal: http://www.regulations.gov.

Comments on the collection of information must be mailed to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW, Washington, DC 20503, ATTN: Desk Officer, United States Coast Guard.

For questions related to TSA's proposed standards, please contact: Rick Collins, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220, TWIC Program, 571-227-3515; e-mail: credentialing@dhs.gov.

5. When will TSA publish the standards for access control devices/readers?

This specification will be in compliance with the FIPS 201-1 standard. It is expected that the detailed access control device/reader documents will be available for release on the web in July.

6. What can I do to prepare for national implementation of TWIC?

TSA and the Coast Guard strongly encourage all interested parties to read the NPRM and provide comments or questions to the addresses listed above in question #4.

7. When will TWIC be implemented at my port?

A final schedule for implementation at specific ports has not yet been determined. In the NPRM, we propose a staggered rollout for enrollment of the current population:

- Group 1: Effective date of rule. Not later than 10 months after effective date of rule.
- Group 2: After Group 1. Not later than 15 months after effective date of rule.
- Group 3: After Group 2. Not later than 18 months after effective date of rule.

A proposed list of ports that may serve as enrollment sites is available at www.tsa.gov/twic under "Links". We are requesting comment on this approach.

8. Who is required to hold a TWIC?

The NPRM proposes that any individual who needs unescorted assess to a secured area of a maritime facility or vessel would have to apply for and hold a TWIC.

9. What will I use my TWIC for?

As currently envisioned, a TWIC would be used to gain access to secure areas of facilities and vessels Owner/operators of facilities and vessels would determine who may have access to the site once a TWIC is issued to the worker.

10. Will my TWIC be compatible with FIPS 201 cards to be issued to Executive Branch employees and contractors?

As currently proposed, TWIC would be compatible with FIPS – 201.

11. Can I use my TWIC to get into any port?

Each owner/operator will determine who is granted access once a TWIC has been issued by TSA.

12. What information will be stored on the card?

As currently planned, the credential will hold a digital photograph, name, TWIC expiration date, fingerprint templates of 2 fingers, finger pattern templates of 2 fingers, a personal identification number, and a Federal Agency Smart Credential number."

13. What are the criminal offenses that would disqualify someone from receiving a TWIC?

Under the proposed rule, section 1572.103, there are two types of disqualifying criminal offenses: Permanent and Interim.

(a) Permanent Disqualifying Criminal Offenses

An applicant would be disqualified if convicted or found guilty by reason of insanity, in a civilian or military jurisdiction of any of the following felonies:

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 State law that is comparable, or conspiracy to commit such a crime.
5. A crime involving a transportation security incident.
6. Improper transportation of hazardous material.
7. Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, dealing in an explosive or explosive device.
8. Murder.
9. Conspiracy or attempt to commit the crimes in paragraphs (a) (5.) thru (8).
10. Violations of the Racketeer Influenced and Corrupt Organization Act (RICO) if a predicate act involves murder or a crime listed in 18 U.S.C. 113B..

(b) Interim Disqualifying Criminal Offenses.

An applicant is disqualified if convicted, or found not guilty by reason of insanity in a civilian or military jurisdiction within the 7 years preceding the date of application, or was released from incarceration for the crime within the 5 years preceding the date application, of the following crimes:

1. Assault with intent to murder.
2. Kidnapping or hostage taking.
3. Rape or aggravated assault.
4. Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon.
5. Extortion,
6. Dishonesty, fraud, or misrepresentation, including identity fraud.
7. Bribery.
8. Smuggling.
9. Immigration Violations
10. Violations of RICO.
11. Robbery.
12. Distribution of, possession with intent to distribute or importation of a controlled substance.
13. Arson.
14. Conspiracy or attempt to commit the interim crimes.

14. What's the difference between a waiver and an appeal?

A waiver is for individuals who clearly have committed a disqualifying criminal offense or have been declared mentally incompetent, but believe they are rehabilitated to the extent that they should be granted a TWIC anyway. TSA reviews waiver requests and grants or denies them on a case-by-case basis. Waiver applicants must complete a security threat assessment so that TSA can review all available criminal history records in making the determination. The TSA website provides guidance on the material waiver applicants should submit, including a summary of the circumstances of the

crime; letters of reference from employers, clergy and probation officers; any restitution made; and any other information indicative of the applicant's rehabilitation.

An appeal is available to all applicants if they believe TSA has not applied the standards appropriately, or has based its security threat assessment determination on incorrect court records or mistaken identity. Applicants who file an appeal may supply the corrected records to TSA or show that TSA has misidentified them.

15. How much will the TWIC cost and who pays for a TWIC?

The proposed fee for a TWIC is expected to range from $105 (MML, HME, and FAST card holders already comparably vetted by DHS) to $139 for all other applicants." The fee will be collected from the applicant at the time of enrollment. The full fee covers TSA's operational costs to deliver the TWIC program, including all enrollment, security threat assessment and adjudication, (including the waiver and appeal process) card production, program office and information systems costs. The fee does not include the TWIC prototype or other start-up costs to the agency, which were funded from Congressional appropriations.

16. What if I have already been through a security threat assessment for a hazardous materials endorsement?

Workers who have undergone certain comparable checks completed by DHS, including hazmat drivers, do not have to complete another threat assessment. However, these workers would have to enroll, provide biographic and biometric information and pay the corresponding fee to obtain a TWIC

17. How do I apply for a TWIC?

Workers will be given information concerning where the enrollment sites are and when enrollment will begin when we publish the final rule. Generally, all workers will be able to 'pre-enroll' on line where they may fill out the enrollment application with biographic information and schedule an appointment at the enrollment center to complete the process. At the enrollment center, applicants will receive a privacy notice and consent form, by which they agree to provide personal information for the security threat assessment and credential. Also, applicants must provide ten fingerprints and sit for a digital photograph, which are electronically captured at the enrollment center for use on the credential. Workers must also provide proof of identity when enrolling.

18. How is my personal information protected?

TSA has designed the TWIC process to maintain strict privacy controls so that a holder's biographic and biometric information cannot be compromised. For a full description of the process, please read the Privacy Impact Assessment for TWIC, which is available for review at: http://www.dhs.gov/interweb/assetlibrary/privacy_pia_tsa_twicnprm.pdf

19. Who will be aware of the results of my security threat assessment? Will this information be given to my employer?

TSA will not give any employer information gathered during the security threat assessment of an employee. Where TSA determines that an imminent threat exists and denies a worker a TWIC, TSA may notify the employer that the worker was denied a TWIC, but would not provide any additional information as to why the TWIC was denied.

20. Do I have to be a citizen to hold a TWIC?

No. Generally, you must be in the United States lawfully and be authorized to work in the United States to pass the immigration status check proposed in the TWIC NPRM. Specifically, in the NPRM we are proposing to permit the following individuals to obtain a TWIC:

--citizens
--lawful permanent residents
--lawful non-immigrants with unrestricted employment authorization
--refugees with unrestricted employment authorization
--aliens granted asylum with unrestricted employment authorization
-- CDL holder licensed in Canada or Mexico who is admitted to the US in 8 CFR 214.2(b) (4)(i)(E) to conduct business in the US

21. If I participated in the Prototype Phase of TWIC and received a credential then, do I need to go through enrollment again and get a new TWIC?

Yes, you must enroll again and receive the fully operational TWIC. We were testing a variety of technologies and processes during Prototype and were not conducting a full security threat assessment on the volunteers. Therefore, you must go through enrollment for the full TWIC program and receive the new credential when directed to by the facility/vessel you work at or need to enter.

22. What are the procedures if disqualifying information is discovered during a security threat assessment and will the applicant be subject to immediate suspension?

Typically, if TSA discovers disqualifying information in the course of a security threat assessment, TSA would notify the applicant by letter with an 'Initial Determination of Threat' and provide the applicant instructions on how to appeal the Initial Determination. In the appeal, applicants may request copies of the material on which TSA made the Initial Determination and provide information to TSA showing that the Initial Determination is inaccurate. If TSA's Initial Determination was issued in error, TSA withdraws the Initial Determination and the applicant would receive a TWIC. If TSA's Initial Determination stands, TSA would issue a Final Determination of Threat and deny the applicant a TWIC. Therefore, the applicant could not access secure areas of maritime facilities or vessels unless under escort. TSA proposes to notify the Federal Maritime Security Coordinator (FMSC) or Captain of the Port (COTP) if the applicant is denied a TWIC and would notify the Coast Guard if the applicant is a mariner.

If TSA determines that an applicant poses an imminent threat to security, TSA would issue an Initial Determination of Threat and Immediate Revocation, and the applicant would be denied the TWIC immediately. The applicant would have the opportunity to appeal TSA's decision following the denial of the TWIC. In cases where TSA believes there is an imminent threat, TSA may notify an employer.

23. What will the security threat assessment include?
TSA proposes to conduct a check of the FBI's fingerprint-based and name-based criminal history records, immigration status, and relevant intelligence and international databases.