TWIC Regulations and Their Impact on Port Facilities

AAPA SUMMARY

PUBLIC COMMENT

Comments to the Record due on July 6, 2006.

Public Meetings: May 31, Newark; June 1, Tampa; June 6, St Louis; June 7, Long Beach.

ISSUANCE OF THE CARD

The program is expected to cover 750,000 workers and would be funded through user fees. TSA anticipates that each worker would pay approximately $139 to receive a TWIC. Workers with current, comparable background checks would pay approximately $105 for the credential. A TWIC card would be valid for five years.

TSA or its agent will do the enrollment. TSA would collect worker's biographic and biometric information, including ten fingerprints; name; date of birth; address and phone number; alien registration number (if applicable); photo; employer; and job title. The TWIC card will include only two fingerprint templates.

TWIC would utilize Smart Card technology and include a worker's photo, name, biometric information and multiple fraud protection measures. The card would be consistent with Homeland Security Presidential Directive-12 and Federal Information Processing Standards Publication 201-1 requirements and would be interoperable with other federal credentials built into those standards.

There will be phased enrollment with centers established based on risk assessment and cost/ benefit analysis. Locations that are considered critical and provide the greatest number of individual applicants will be among the earliest enrollment sites. Fixed and mobile centers will be used. There will be 125 locations for 300 ports. Comments on the locations of the enrollment center are welcome and will eventually be listed on www.tsa.gov.

Three phases are proposed for the timeframe for enrollment. This is the timeline only for doing the background check. Issuance of the card may take an additional 30 days. There will be coordination with the Captain of the Port, and the Area Maritime Committee (AMS) to schedule enrollments to avoid backups. If more time is needed, Coast Guard and TSA will consider this in future rulings.

• Group 1	10 months from effective date
• Group 2	15 months from effective date
• Group 3	18 months from effective date

Comments on how to notify employers of denied TWICs is also requested. TSA is proposing that it will notify an applicant's employer, where appropriate, when issuing final determinations of threat assessments or immediate revocations. TSA is considering establishing a secure web site for employers to list employees with TWIC, but would like comments on this. The TWIC application will ask the individual to list the employer and it notifies them that the employer may be notified if there is a denial. TSA will also notify the Federal Maritime Security Coordinator who is the Captain of the Port of any denials.

CRIMINAL / IMMIGRATION BACKGROUND CHECKS

All TWIC holders must undergo a background check to review of criminal history records, terrorist watch lists, legal immigration status and outstanding wants and warrants. It is similar to the system used for hazardous materials drivers. State criminal databases will not be checked, only FBI criminal databases.

The MTSA states that an individual can be denied a card if they have been convicted within the preceding seven-year period or released in the last five years of a felony or found not guilty by reason of insanity of a felony that DHS believes could cause the individual to be a terrorism security risk to the U.S. or for causing a severe transportation security incident. The law does not specify those crimes. The law also noted that a TWIC may be denied for immigration violations or other terrorism risks.

The proposed rule proposes what those violations should be. For permanently disqualifying criminal offenses crimes and conspiracy to commit they list:

- espionage; sedition; treason; a terrorism crime, a transportation security incident crime, improper transportation of hazardous material; unlawful possession, use, sale, …or dealing in an explosive or explosive device; murder; or violations of RICO (organized crime).
- Those who have been involuntarily committed to a mental institution are considered to pose a security threat and will be disqualified.

There also are 14 crimes that would disqualify an individual if they were convicted within seven years or incarcerated within five years. These are:

- assault with intent to murder;
- kidnapping or hostage taking;
- rape or aggravated sexual abuse;
- unlawful possession, use, sale….of a firearm or other weapon;
- extortion;
- dishonesty, fraud, or misrepresentation, including identity fraud;
- bribery;
- smuggling;
- immigration violations;
- lesser RICO violations;
- robbery;
- distribution, possession with intent to distribute, or importation of a controlled substance, including drugs;
- arson and
- conspiracy.

If an applicant has been imprisoned for more than one year and did not commit a crime listed above, TSA may still deny a TWIC.

TSA proposes to add a new paragraph on immigration standards for TWIC applicants to permit certain drivers licenses in Canada or Mexico who frequently deliver goods to facilities and vessels to meet the immigration standards for holding a TWIC. These drivers are admitted to the U.S. under the NAFTA implementation visa category.

INDIVIDUAL REQUIREMENTS

All mariners with active Licenses, Merchant Mariner Document or Certificate of Registry and all persons who need unescorted access to a MTSA facility or vessel must have a TWIC. This includes longshoremen, port operator employees, truck drivers and rail workers.

All individuals with security duties for an MTSA-covered facility or vessel, including the company security officer, must acquire and maintain a TWIC. The Coast Guard is asking for comments on whether owner/operators should also be required to obtain a TWIC based on their access to sensitive security information.

All Area Maritime Security (AMS) Committee members will have to hold a TWIC or have passed a comparable security background investigation, with the exception of credentialed federal, state and local officials.

Federal and state officials would not be required to use the TWIC, but would use their HSPD12-compliant agency credential.

Applicants may pre-enroll but need to go to the enrollment center for biometric fingerprints (10), a digital photo, verification of their identity, and to sign documents. They need to explain why they need a TWIC and may be required to provide a job description.

TSA is welcoming comments on how to notify individuals of TWIC acceptance or denial. Should they allow email notification? How should employers be notified?

Individuals must return to the enrollment center to pick up their TWIC and select a PIN. TSA welcomes comments on alternatives to returning to the enrollment center. There is no mention on how to reset or get a copy of a PIN if an individual can not remember it. During security level MARSEC III, individuals must present a card and a PIN to gain access to a facility and the PIN can be used for an alternative security metric.

If denied, an applicant must appeal in a set amount of time. TSA is proposing 60 days for a written appeal, which must include evidence that the Initial Determination was incorrect.

Applicants with certain disqualifying offenses or issues of mental competence may apply for a waiver. Waivers are offered because an applicant may be rehabilitated to the point that he or she can be trusted.

Applicants must return to the enrollment center after five years to renew the card, providing the same biographic and biometric information and pay the associated fees. They will not receive notification that their TWIC needs to be renewed because the date is on the front of the card. Renewals must begin 90 to 180 days before expiration.

To replace a lost, stolen or damaged card, an applicant must return to the enrollment center. Lost or stolen cards need to be reported immediately to a call center. There is a $36 charge to replace a card. During the protype phase, cards were ready within 24 hours.

FACILITY REQUIREMENTS

A full list of facility requirements: Summary P 29412 33 CRF part 105, and full text can be found on page 29443 - 45 of FR May 22 Proposed Rules.

Facility owner must notify workers of their responsibilities to enroll and the deadline for doing this. At least 60 days out individuals should apply for a card. TSA will give owners/operators a list of enrollment facilities to give to individuals who need to apply for a TWIC.

The TWIC rule is performance-based. Facility/vessel owners determine which TWIC holders will be granted access to secure areas of their facility, but would be required to implement TWIC into their existing access control systems and operations, purchase and utilize card readers, and update their approved security plans. Access control procedures and systems at facilities and vessels must recognize the credential and the information encrypted on it, so that the overall maritime network will be interoperable.

Facilities would have six months from the date of the final rule to submit a TWIC addendum to their COTP and would be required to be operating according to the addendum within 12 and 18 months depending on whether enrollment has been completed at the port where the facility is located.

TWIC depends on three factors to establish a person's identity. This process consists of identifying:

1) something the person has – a TWIC credential
2) something the person knows – a PIN
3) something the person is – a fingerprint.

For unescorted access the person must have a TWIC that is electronically verified against his or her identity by matching his or her biometric against the information stored on the credential. In addition the owner/operator would have to confirm that the TWIC remains valid. Workers will not be allowed to "flash" their card as identification.

The access control administrator must verify that the individual holding the TWIC matches the biometric stored on the TWIC by conducting a one-to-one match with the individual's finger and fingerprint template stored on the chip in the TWIC. The operator verifies that an individual's TWIC is valid, either by directly interfacing with the TSA system or by using a list of invalid credentials downloaded from TSA. How often the facility owner must check against the TSA database varies based on the current MARSEC level. Facilities must ensure within 12 hours of notification of an increase in MARSEC Level that is implementing the additional security measures required for the new MARSEC level and their plan.

- For MARSEC 1 –Requirements include one-to-one biometric match and verification against the latest information from TSA on a weekly basis.
- For MARSEC 2 – Owner/operators would be required to complete the one-to-one biometric match and ensure that the validity of TWIC credentials are verified against TSA data on a daily basis, and may increase other access control measures as specified in their port security plan. Cruise ships will have stricter requirements as MARSEC 2 – they must check the biometric and enter a PIN and have information validated with the most current information available from TSA.
- At MARSEC 3, there is a biometric match and a PIN is required and validation is based on information equal or less than one day old. Facilities also should implement additional access control measures as specified in their plan.

The owner/operators may opt to notify TSA that access privileges have been granted to a worker. If this option is invoked, owner/operators must also notify TSA if it denies access for some reason.

Specific requirements for access control measures are located on page 29444 section 105.255.

Facilities may determine where the card readers are located, the details of the access control system and the system used to resolve access problems. Facilities must ensure that security systems and equipment are installed and maintained, including at least one TWIC reader that meets the standard incorporated by TSA in 49 CFR 1572.23, and that computer and access control systems and hardware are secure. The Coast Guard’s docket includes a sample document on this and requests comments on the proper standard of care to be used to protect these systems and hardware.

Facilities must have a backup process for making access control decisions should any part of the TWIC system fails and security personal must be trained in this system at all entry points.

If owner/operators choose to use a separate badge system, it must be coordinated with the TWIC requirements, such that notification to the owner/operators of changes in the individual’s TWIC status are also reflected in the separate badging system.

Facilities may need to adhere to stricter state regulations regarding access to a facility.

The Coast Guard is proposing adding knowledge requirements and responsibilities pertaining to TWIC to those already assigned to owners/operators, facility security officers, facility employees with security duties, and all facility employees. There will be no formal training requirements in order to meet the TWIC knowledge requirements. These requirements relate to:

- Alternate ways to reliably verify an individual’s identity.
- All employees should be familiar with the TWIC topology, as well as the steps to take should their own TWIC become lost or stolen.

A new requirement is established that owner/operators must ensure that someone within the facility knows who is in the facility at all times.

Owner/operators must keep records for two years of all persons granted access to the facility. For escorted access, the owner/operators would be required to record each date that the individual is escorted and identify his/her escort.

Certain incidents involving a TWIC as either a suspicious activity or breach of security — such as a person trying to gain entry using an invalid TWIC, or if a person without a TWIC if found in the secure area — should be reported to the Coast Guard. If an owner/operator knows of a reason that an individual who holds a TWIC should have it revoked, they should report it as well.

Facilities are only required to deny unescorted access to an individual who attempts to access a facility with a TWIC that has been revoked. If they believe there is a problem with the card, the owner/operator is required to immediately report the matter to Coast Guard or local law enforcement.

Vessels that are exempt from the MTSA requirements are exempt from TWIC. There are no changes at this point to the regulations on how crews get on and off ships, but that may be addressed in future rules. Facilities must coordinate with vessels and address this issue in their security plan.

For cruise facilities a new requirement is listed that states facilities must check the identification of all persons seeking to enter the facility. Persons holding a TWIC shall be checked. For persons not holding a TWIC, this check includes confirming the reason for boarding by examining passenger tickets, boarding passes, government identification or visitor badges, or work orders.

AREA MARITIME SECURITY COMMITTEES (AMS)

AMS Committee members may serve a maximum of five years.

All AMS plans must address biometric access programs within the port, and the AMS plans must be updated to reflect compliance with TWIC regulations.

Elements of an AMS plan must also include security measures designed to ensure the effective security of infrastructure, special events, vessels, passengers, cargo and cargo handling equipment at facilities within the port not otherwise covered by vessel or facility plans.

IMPACTS

The regulation states that there are no significant barriers to international trade, no unfunded mandate on state, local or tribal government and no unknown impact on small business.

The start-up costs plus initial enrollments cause roughly 40% of expenses to occur in the first year. Total cost over 10 years is $1,028 million. Facility costs account for about 39% of the estimated costs. The cost for facility implementation would be between $299 and $325 million.

Page 29435 outlines the cost of implementation for small businesses.

- Smart card reader purchase - $2,000-$5,000
- Smart card reader software - $1000
- Smart card reader installation - $200
- Creating TWIC addendum - $1,693
- Knowledge Requirements - $2,709
- TWIC validation - not listed
- TOTAL: $8,906-$11,093

OTHER

New requirements are proposed for cruise and ferries that would have a significant impact on the way that owners and operators make access control decisions.

Comments are being sought regarding whether the TWIC program should be extended to other areas in the transportation industry outside of the maritime sector, such as rail, mass transit, pipeline, and aviation.