

QUESTIONS:

- 1) What are your recommendations regarding the number of individuals in a vessel's crew that would warrant the placement of a TWIC reader onboard?

On a container ship the size of the crew is not the big factor as opposed to a tanker or other type of vessel.

- 2) What factors, in addition to crew size, do you feel should be considered during the development of proposed regulations which might require card readers to be placed onboard vessels?

Containership may have 25-30 vendors, 15-20 visitors, and 50-75 longshoremen come up the gangway during a port stay. Having a TWIC reader onboard would enable the vessel to accurately reflect how many of these people are onboard at any given time. This has been mandated by U.S. West Coast COTPs and at this juncture we have difficulty meeting this requirement with a manual signing in and out process.

- 3) What factors, in addition to crew size, do you feel would warrant an exception to the requirement that a card reader be placed onboard a vessel?

No exception.

- 4) If card readers are not required to be placed onboard certain vessels, what recommendations would you propose for the Coast Guard to consider regarding the location or operation of card readers to accomplish TWIC validation?

TWIC readers at the gates to terminals will control access onto the marine facility however; they will not control access between vessels.

- 5) For these specific vessels, would it be more convenient and practicable to use card readers at a company's home or field office?

This will do nothing for controlling vessel access.

- 6) What recommendations can you provide for the Coast Guard to use when drafting the proposed regulations, regarding the type and frequency of checks using card readers for these specific vessels?

TWIC Reader should be used every time an individual goes on and off the vessel. There should be a test card for ensuring that unit is properly calibrated and reading. Any false readings should be verified with backup ID.

Regarding the installation and use of electronic readers aboard MTSA regulated vessels and facilities (including OCS facilities regulated under 33CFR106), the original NPRM published on May 22, 2006, proposed electronically verifying TWICs prior to granting unescorted access upon each entry, except for vessels utilizing recurring unescorted access. The NPRM also proposed varying levels of TWIC validation based on the

current MARSEC level and other factors. The following security checks should be available to the owner or operator while conducting an electronic verification of the TWIC:

- a) Hot List Check – The process of verifying the card would include comparing the TWIC Card Holder Unique Identification (CHUID) number against the TSA-published list of revoked cards (hot list). This is necessary to ensure that cards remain valid and have not been revoked for security reasons after initial issuance. TSA plans to make the hot list available electronically, via the internet or some other open source, to facilitate downloading and use by reader operators in the maritime industry.
- b) Display of Digital Photograph and Name – The contact (open slot) reader should be capable of accessing the name of the individual and the digital facial image stored within the credential. The reader should be capable of displaying the image for manual comparison against the image visible on the face of the card and the TWIC holder.
- c) Digital Signature Check – The card reader, regardless of if it is contact or contactless, should be capable of accessing the digital signature stored within the credential to ensure the credential is authentic.
- d) Personal Identification Number – While use of the PIN will not be required when checking TWICs using a contactless reader, it will be required to be entered and matched to the PIN stored within the credential to unlock and transfer data using a contact (open slot) reader. Manual entry of a PIN provides a certain level of security and privacy in that only the authorized holder of that particular TWIC should know it.
- e) Biometric Match – The card reader should be capable of matching the fingerprint (biometric) of the TWIC holder to the biometric template stored within the credential. This match provides a higher level of security and assurance that the TWIC holder is the rightful owner of the credential.

QUESTIONS:

- 7) Under what circumstances would you recommend that not all of the available security features be checked? In other words, why shouldn't all of the available security features be checked when using a card reader for each individual gaining unescorted access to secure areas?
 - a) The verification of crew against a hot list would have to be done at the home office as our vessels do not have direct access for downloads. Vendors coming onboard the vessel would go through the hot list check prior to gaining access to the facility.
 - b) Don't understand the question.
 - c) Don't understand the question.
 - d) The entering of a PIN each and every time an individual attempts to gain unescorted access to secure areas is unrealistic, does not provide added

security given the degree of difficulty of this exercise and will adversely impact the flow of trade.

- e) Matching of the fingerprint of the TWIC holder to the biometric template stored within the credential should only be done at MARSEC levels 2 and 3.

- 8) Do you feel that the frequency of electronic validation should be based on unique vessel or facility types, operations, and activities? What factors should be considered when developing proposed requirements for the frequency of electronic validation?

The frequency of electronic validation should be based on vessel type. Vessels should be rated from highest to lowest priority as follows: LNG/LPG, Cruise/Ferry, Chemical Tanker, Tanker, Bulk (CDC), Container, Bulk (non-CDC).

- 9) What factors should be considered when developing proposed regulations regarding the required frequency for updating card readers or card reader systems with the most current version of the TSA hot list?

The frequency of updating card readers or card reader systems with the most current version of the TSA hot list should increase as the MARSEC level increases.

Other factor to consider:

- Who is authorized to handle this data as this may be considered SSI material?

- 10) What issues and options should be considered when drafting proposed regulations to enable vessels without internet connectivity to ensure TWICs have not been revoked? Could this be accomplished at a home or regional office on behalf of a vessel while underway?

The TWIC validity of crewmembers and vessel vendors should be screened by the home office.

- 11) If the types of checks to be conducted while using a card reader are based on risk and current MARSEC level, which of the security features listed in the preamble to questions 7-12 could be checked on the lowest risk vessels or facilities with a minimal impact on commerce, throughput and daily operations?

Display of Digital Photograph and Name should be checked on the lowest risk vessels or facilities.

- 12) Which of the following would be most effective in discovering if TWICs have been hot-listed? Can you provide recommendations or other options for ensuring TWIC's have not been hot listed?

- a) Privilege Granting: The owner/operator communicates directly with TSA the name of TWIC holders granted unescorted access to secure areas of their vessel or facility. In the event that a TWIC has been revoked, the

owner or operator would be contacted by TSA and informed that the TWIC is no longer valid. If an individual is employed aboard multiple vessels or facilities with different owners/operators, all vessels or facilities would have to be on file with TSA in order for TSA to make contact with them in the event of an invalidation.

- b) Downloading the hot list: The owners/operators would be responsible for ensuring their card readers contain the most recent version of the TSA hot list on a scheduled basis, for example, by MARSEC level or type of operation, to be used when checking TWICs to meet the validity check requirement.
- c) Manual Checks of the hot list: The owner/operator would manually compare the TWIC CHUID number against a published list of CHUID numbers on a scheduled basis, for example, by MARSEC level or type of operation.

This is far too complicated and complex to respond to without additional information and supporting data.

- a) It would depend on the vessel's capability to communicate to TSA the names of all TWIC holders granted unescorted access to secure areas.
- b) Depends on the quantity of individuals on the hot list and the availability of effective technology to achieve the download.
- c) Manually checking of any list is cumbersome and the impact on operations would depend on the size of the hot list.

The Coast Guard is also considering record keeping requirements similar to those proposed in the May 22, 2006 NPRM. The security benefits of knowing who is granted unescorted access and who is aboard a facility or vessel at all times, will enhance security by providing improved situational awareness. This is especially valid for larger facility operators who may have hundreds or even thousands of personnel on their property at any given time. It is expected that the electronic card readers will be capable of automating this process with little or no additional effort by the owner or operator. If TWIC readers were employed to accurately track who is aboard a vessel or within a facility's secure area at any given time, then TWICs would also have to be read upon departure from the vessel or secure area.

QUESTIONS:

- 13) Under what conditions should an exception be granted to the requirement that records be maintained for individuals who are currently in a secure area or who have been granted unescorted access to a facility or vessel?

Emergency situations for emergency personnel such as firemen, law enforcement, as well as persons with TWIC Cards who have emergency duties. Supervisors should have muster lists of who was present and these should be provided to security personnel when time allows.

14) If you disagree with the concept of proposing record keeping requirements for individuals granted unescorted access to secure areas of a vessel or facility, what alternate system or measures would improve the situational awareness of who has unescorted access?

None.

15) What requirements should there be for keeping records on individuals who have been granted *escorted* access to secure areas?

The visitor log book, where the individual without a TWIC must show security ID and sign in before being granted escorted access, should be maintained for six months.

The existing TWIC regulations clearly indicate that each vessel or facility is responsible for its own access control. The vessel – facility interface may offer some options to reduce the effort and number of times an individual’s TWIC needs to be checked using a card reader.

QUESTIONS:

16) What suggestions do you have regarding the Coast Guard’s proposed requirements that a TWIC be checked using a card reader each time an individual boards a vessel while it is moored at a regulated facility? What if the TWIC were checked only when an individual enters the facility?

As previously stated manual logging in system is onerous, prone to mistakes, difficult to enforce, and slows work force down. TWIC reader is none of these and will easily provide access control as well as accurate up to the minute information about who is on or off the vessel. The checking of TWIC only when an individual enters the facility does not address the issue of crewmen getting off a vessel and going onto another vessel.

17) Do you feel that the answer to question 16 above should be the joint responsibility of the facility and vessel on a case-by-case basis? Or, should each regulated entity be responsible for validating TWIC’s prior to granting unescorted access to its own secure areas? In the event that the responsibility be a joint one, should this agreement be documented in a Declaration of Security?

Each regulated entity should be responsible for its own secure areas.

The Maritime Transportation Security Act (MTSA) also requires that “all vessel pilots” [46 U.S.C. 70105(b)(2)(C)] and “all individuals working aboard towing vessels that push, pull or haul alongside tank vessels” [46 U.S.C. 70105(b)(2)(D)] hold a TWIC.

Although no specific regulation requiring “all vessel pilots” was included in the final rule, the majority currently hold a Coast Guard license and will be required to obtain a TWIC due to their status as a credentialed mariner. We are considering proposing regulations to require that the remaining pilots, those few holding state commissions or credentials but not a Federally-issued merchant mariner license or document, obtain a TWIC.

Regarding “all individuals working aboard towing vessels that push, pull or haul along side tank vessels,” the current TWIC regulations require only credentialed mariners, vessels subject to 33 CFR Part 104, and those individuals who need unescorted access to secure areas to comply with TWIC regulations. In order to comply with the statute, we are considering proposing a requirement to address the issue of all individuals working aboard non-Subchapter H regulated towing vessels that push, pull or haul alongside tank vessels. These are towing vessels less than or equal to eight meters in registered length and some larger towing vessels that meet the exemptions listed in 33 CFR 104.105.

QUESTIONS:

18) Do you have any suggestions on how to address these populations in the TWIC 2 regulations?

If one class of workers is exempted then security risk increases for all, there should be no exceptions.