

TOWING SAFETY ADVISORY COMMITTEE (TSAC)
TASK STATEMENT

TASK #07-01

I. **TASK TITLE**

Feedback for Preliminary Draft of the Transportation Worker Identification Credential (TWIC) Biometric Reader Requirements Notice of Proposed Rulemaking (NPRM).

II. **BACKGROUND**

The Transportation Security Administration (TSA) and the Coast Guard published a Notice of Proposed Rulemaking on May 22, 2006, proposing TWIC requirements to meet the mandate of the Maritime Transportation Security Act (MTSA) of 2002. MTSA requires members who have unescorted access to secure areas of maritime facilities and vessels to possess a TWIC. The NPRM indicated that the TWIC will be aligned with the Federal Information Processing Standards 201-1 (FIPS-201), and proposed card reader requirements for the use of TWIC for access control to secure areas.

During the public comment period of the rulemaking, numerous concerns were raised regarding card readers, including uncertainty on costs, specifications, connectivity, and application. In addition, concerns were voiced that the FIPS-201-1 specification did not allow for contactless use of a TWIC. This would result in the procurement of contact card readers, which would not be sufficiently durable for use in the maritime environment. After careful deliberation on all of the comments, TSA and the Coast Guard announced on August 21, 2006 that the requirement for card readers would not be included in the TWIC Final Rule. Instead, a follow-on rulemaking would be initiated to separately address requirements for the use of card readers for access control to secure areas.

On October 13, 2006, the SAFE Port Act, which contained specific provisions for the TWIC program, became law. It requires, among other things, that the Department of Homeland Security conduct a TWIC pilot program in five distinct locations to test the business processes, technology, and operational impacts required to deploy TWIC readers. The results of this pilot program will be used in the second TWIC rulemaking (hereafter referred to as TWIC 2), which is intended to incorporate contactless card reader capability to meet the demands of TWIC application in the maritime environment. A second rule requiring “the deployment of transportation security card readers that are consistent with the findings of the pilot program,” with the final regulations of which must be promulgated “not later than 2 years after the commencement of the pilot program” was also specified by the SAFE Port Act. Although this timeline seems distant, it is important to continue on an aggressive

schedule to establish TWIC reader requirements and gain the full security benefit that the TWIC provides as soon as possible.

III. PROBLEM STATEMENT:

In order to obtain the best information to improve the development of the TWIC2 NPRM, the Coast Guard is requesting assistance from the Towing Safety Advisory Committee (TSAC). TSAC's input is critical to the successful early drafting stages of this important NPRM.

IV. TASK:

Assist with the development of the draft Transportation Worker Identification Credential (TWIC) Biometric Reader Requirements Notice of Proposed Rulemaking. We request that any comments or recommendations be submitted to your Committee Sponsor no later than July 23rd, 2007 in order to assist the Coast Guard in clearing the draft NPRM this summer.

V. ESTIMATED TIME TO COMPLETE TASK

The Committee should provide its findings and recommendations to the Coast Guard by 17 July 2007.

VI. COAST GUARD TECHNICAL REPRESENTATIVES

CDR Peter Gautier, Chief, Coast Guard Facilities and Cargo Division, CG-3PCP-2, 202-372-1171, Peter.W.Gautier@uscg.mil

LCDR Jon Maiorine, Chief, Security Standards Branch, CG-3PCP-2, 202-372-1133, jonathan.h.maiorine@uscg.mil

Enclosure (1): Transportation Worker Identification Credential (TWIC) Biometric Reader Requirements Notice of Proposed Rulemaking - Advisory Committee Questionnaire

**Transportation Worker Identification Credential (TWIC) Biometric Reader Requirements
Notice of Proposed Rulemaking - Advisory Committee Questionnaire**

In response to numerous comments and suggestions received during the public comment period from May 22nd, 2006 to July 6th, 2006, the Coast Guard desires to continue utilizing a risk based approach during the development of reader requirements for the proposed rule, (hereafter referred to as TWIC 2.) A fundamental approach to reducing risk is to reduce vulnerability. The requirement for any specific vessel, facility, operation or activity to employ and utilize TWIC readers will reduce vulnerability by providing a greater level of assurance that individuals granted unescorted access to secure areas hold a valid TWIC, and have passed a security threat assessment. While use of the TWIC as a “flash pass” provides an initial degree of security, as it serves as a standard, tamper resistant identification card which is only issued after an individual passes a security threat assessment, only through the use of electronic readers can the credential’s full security features be utilized, and full risk reduction benefits be gained. Electronic readers will enable the owner or operator to conduct a biometric match of the holder to the template stored on the card, to ensure the TWIC has not been revoked (or “hot listed”), and to ensure the TWIC contains an authentic digital signature (i.e. ensure that the TWIC was issued by TSA).

Additionally, the SAFE Port Act of 2006 specifically states that “the Secretary may not require the placement of an electronic reader for transportation security cards on a vessel unless –

“(1) the vessel has more individuals on the crew that are required to have a transportation security card than the number the Secretary determines, by regulation issued under subsection (k)(3), warrants such a reader; or

“(2) the Secretary determines that the vessel is at risk of a severe transportation security incident.”

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?

At a minimum, vessels with a total required crew complement of 14 or fewer – or fewer than 14 individuals holding a TWIC -- should not be required to have a card reader on board. (Per NVIC 03-07, for a vessel with a COI, “required” crew includes all personnel in the required manning section; for a vessel without a COI, “required” crew includes all personnel performing navigation, safety, and security functions.)

Exemptions for vessels with larger crews should also be considered, as discussed in response to the questions below. However, no vessel with a required crew of 14 or fewer, or 14 or fewer individuals requiring a TWIC on board, should ever be required to have a card reader on board.

- 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?

Other factors that should be considered include the number of personnel who will be boarding the vessel or seeking access to secure areas at any given time (the smaller the number, the more easily the TWIC can be used as a “flash pass” in lieu of requiring a reader); access control procedures included in the vessel’s Vessel Security Plan or Alternative Security Program; and arrangements with the facility(ies) served by the vessel (including the presence/use of card readers at the dock or other appropriate shoreside location).

- 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?

Vessels with crew sizes greater than 14 should not be required to have a card reader if: 1) no more than a specified number of individuals will be boarding the vessel or accessing secure areas at any given time; 2) the vessel owner’s VSP or ASP includes alternative procedures for access control appropriate to the vessel’s size, operations, and risk profile; or, 3) the vessel owner enters into an arrangement with the owner(s) of facilities served by the vessel to use card readers installed at the dock or other appropriate shoreside location.

- 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?

The location of card readers should be determined by the facility owner as part of the Facility Security Plan or Alternative Security Program.

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

Owners of vessels that are not required to have card readers onboard should not be required to use card readers for the purpose of TWIC validation (although they should have the option of using a shoreside reader for this purpose if they choose). Validation of TWICs by vessel owners can be accomplished by checking the hotlist of expired/revoked TWICs as discussed below.

The location of card readers used for access control should be determined by the facility owner as part of the FSP or ASP.

- 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?

As discussed in question 5 above, the use of card readers for TWIC validation should not be required for vessels that are not required to have card readers on board.

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?

Checks a) and c) (hot list check and digital signature check) should be required at all MARSEC levels when using a card reader for access control. Checks b) (display of digital photograph and name) and e) (biometric match) should only be required at MARSEC 2 or higher when using a contact card reader. The personal identification number should never be

required for access control as PINs can easily be forgotten. Routinely requiring checks other than a) and c) at MARSEC 1 will add unnecessary time and complexity to the process of accessing a vessel or facility. (Of course, a facility owner should have the option to conduct all the checks at MARSEC 1 if he/she so chooses, but this should not be required by the Coast Guard.)

- 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 Coast Guard should not require electronic validation of TWICs at a specified frequency. The frequency of validation will depend upon operational factors (i.e., the need for crewmembers to transit secure areas of a regulated facility in order to access the vessel).

The Coast Guard should establish a minimum frequency for verifying that a TWIC is not on the hot list (i.e., it has not expired or been revoked). As discussed below, this may involve, but should not require, the use of a card reader. MARSEC level should be taken into account in determining the frequency of required hot list checks.

- 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?

Factors that should be considered include the frequency with which the hot list will be updated by TSA and the current MARSEC level.

- 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 Coast Guard should not specify where or by whom the check of TWICs against the hot list should be accomplished. The agency should establish a minimum frequency, based on MARSEC level, at which the validity of TWICs will be checked, and then require vessel and facility owners to spell out in their VSP, FSP, or ASP how this will be accomplished. The Coast Guard and TSA should ensure that the hot list is available to vessel and facility owners by Internet and telephone.

For example, suppose the Coast Guard requires that TWICs be verified against the hot list every two weeks at MARSEC 1. A vessel owner's VSP or ASP could specify that every two weeks, the Company Security Officer will download the list of hot-listed TWICs and check it against the TWIC numbers of company employees. The VSP/ASP could then specify the procedures that would be followed if an employee is found to have a hot-listed TWIC (e.g., immediate, secure notification to Vessel Security Officer on the vessel on which the crewmember is sailing, etc.).

- 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?

As recommended in response to question 7 above, checks a) and c) (hot list check and digital signature check) should be required at all MARSEC levels when using a card reader for access control. We assume that these checks can be accomplished by a contactless card reader quickly and with no requirement for additional intervention on the part of the TWIC holder.

- 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 TWICs 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.

All of these options should be made available. In addition, there should be both an Internet and a telephone option by which an employer can quickly check to see if a particular TWIC is on the hotlist. The employer should be able to enter a TWIC number (by computer or by phone) and have it checked against a database of hotlisted TWIC (similar to the Internet or telephone banking process of entering a specific check number to see if it has cleared).

Employers should not be required to check TWICs against the hot list until these options are in place and fully automated.

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?

No additional recordkeeping requirements should be added to those that already exist in the vessel and facility security plan requirements.

- 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?

We believe this issue is adequately addressed under existing vessel and facility security plan requirements and see no need for additional requirements in this regard. This is particularly true for vessels with small crews, such as towing vessels.

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

As indicated in the response to question 13 above, no additional recordkeeping requirements should be added to those that already exist in the vessel and facility security plan requirements.

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?

The location of card readers to control access to a facility should be determined by the facility owner and specified in the facility security plan. If the layout of the facility and the procedures in the facility security plan are such that any individual attempting to gain unescorted access to a vessel has already had his or her TWIC scanned by a reader, there is no reason for the TWIC to be scanned again prior to the individual boarding the vessel. However, because access to the facility does not automatically confer the right to board a vessel moored at the facility, the vessel

security officer will still need to ensure that only individuals authorized to board the vessel are allowed to come on board. Such procedures will be – and already are – spelled out in the vessel security plan and need not include the use of a card reader.

- 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 TWICs prior to granting unescorted access to its own secure areas? In the event that the responsibility is a joint one, should this agreement be documented in a Declaration of Security?

The facility owner retains the responsibility for controlling access to the facility; the vessel owner retains the responsibility for controlling access to the vessel. This should not preclude vessel and facility owners from working together to arrive at mutually acceptable arrangements that can be documented in a Declaration of Security.

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?

The Coast Guard should issue a notice of proposed rulemaking requiring all personnel on towing vessels that push, pull, or haul alongside tank vessels to hold a TWIC. As a practical matter, we do not expect this clarification to increase materially the number of personnel required to hold a TWIC.

Concluding Comments

TSAC appreciates the opportunity to provide feedback on the TWIC 2 rulemaking at this early stage of the regulatory process. However, we are dismayed by the Coast Guard's indication that the agency plans to publish a notice of proposed rulemaking (NPRM) before the pilot program to test TWIC card readers has been conducted. We believe this sequence should be reversed. The Coast Guard should strive to publish the highest-quality NPRM possible by: 1) completing the TWIC reader pilot program and 2) engaging in extensive consultation with stakeholders, including TSAC and other federal advisory committees before a notice of proposed rulemaking is published.

The Coast Guard should use the preliminary feedback provided by TSAC and other federal advisory committees to develop a standard testing protocol – i.e., standard procedures for pilot program participants – for use during the card reader pilot program. The agency can test these procedures, along with the reader technology, during the pilot program, and then use the results of the pilot program to inform the development of the TWIC 2 NPRM.