

National Maritime Security Advisory Committee (NMSAC) Task Statement

Transportation Worker Identification Credential Biometric Reader Requirements - Notice of Proposed Rulemaking

I. Task Title. 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 contribute to 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 information to improve the development of the TWIC 2 NPRM, the Coast Guard is requesting assistance from the Merchant Marine Personnel Advisory Committee (MERPAC), Towing Safety Advisory Committee (TSAC), and National Maritime Security Advisory Committee (NMSAC). MERPAC's, TSAC's and NMSAC'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. Due Date. 23 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?
- 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?
- 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?

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

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?
- 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?
- 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?
- 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?
- 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?
- 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.

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

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?
- 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?

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 alongside 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?