

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?
It is recommended that the number of crew that would warrant the placement of a TWIC reader on board take into account the activities of cruise vessel operations and the number of foreign crew on board that may have difficulty either A) qualifying for a TWIC card or B) are unable to enroll in the TWIC system due to transit schedules and availability to physically enroll and subsequently “pick-up” and “validate” the TWIC card.
- 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?

There is a concern about the eligibility of vessel crew to qualify for a TWIC card, i.e. nationality, disqualifying factors, lack of information and validation of criminal behavior. The ability for the vessel to update their TWIC readers with the latest “hot list” of invalid cards may be a concern for the maritime industry. There may be situations where the MARSEC Level of the vessel varies from the facility at which the vessel moors, creating a disparity on the way the TWIC card is used, either in a “flash pass” configuration or in a full biometric application.

- 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?

A documented U.S. Mariner who has already passed a background check as a condition for the receipt of a Coast Guard issued license or document, should not need to possess yet another credential for access to the vessel upon which he/she works. Additional credentials create the potential for disparity in which document or credential is superior in allowing access to the vessel. Another concern regarding TWIC cards for mariners is the potential delay in reporting and replacement of a lost or stolen TWIC card by a mariner who may not be in a U.S. Port for some extended period of time

- 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?

While unpalatable from a cost and operational standpoint of the facility operator, an alternative to TWIC readers on board the vessels may be a portable weather hardened and intrinsically safe portable TWIC reader that can be “loaned” to a vessel by the Facility if the facility itself falls under the regulatory requirements for the use of TWIC cards. If the facility already requires a TWIC card for access from outside of the secure perimeter into the facility, then the requirement for a TWIC reader for the vessel becomes a moot point, as the facility is already enacting the TWIC program. The argument falls apart should a vessel subject to the requirements for a TWIC reader on board call on a public access facility where TWIC readers and credentials are not required. In such case, it may be advisable for the vessel to possess a portable TWIC reader that can be stationed at points of embark and debark for the vessel.

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

The intent of the question is unclear. If however the question involves the use of a TWIC card as an identification or access credential to non-vessel, non-regulated facilities or offices, then the Port of Seattle recommends not using TWIC cards in this fashion, as it induces additional costs and administration for facilities where heightened levels of security under the TWIC program may not be applicable or necessary. Efforts should be made to keep costs and maintenance of the TWIC program as low as possible. Likewise, there is an

intrinsic security value to keeping the total number of TWIC credentials to the minimum nation wide.

- 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?

The frequency of checks and use of the TWIC cards for access to vessels at MTSA facilities should be kept consistent with what is required of the facility at all MARSEC Levels to avoid potential conflicts and confusion.

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?

It is recommended that the PIN number be eliminated from use. In practice, the Port of Seattle has experienced a significant degree of PIN numbers simply written on the back of the card, negating the security value of the PIN number.

If the PIN number is to be used, it should be used with every transaction to keep familiarity with the number. If personnel do not have to use the PIN number on a regular basis, the PIN number is forgotten in our experience. This necessitates contacting the card issuing agency for re-issue or update of the PIN number data to the card holder, which has its own intrinsic vulnerabilities of validating the person who is requesting the PIN number update is in fact the valid card holder. For those persons who are able to use a biometric, it is recommended that the biometric be substituted for the PIN number, as there is nothing to be forgotten, and nothing to be written down on the back of the card.

The additional time required to enter a PIN number in addition to presentation of the TWIC card to gain access to a high-throughput facility could be a significant issue to some facilities.

- 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?

It is recommended that a schema of electronic validation that provides for the greatest consistency and least amount of confusion. At the most simplistic level, use of electronic validation for all entry to facilities where a TWIC card is required keeps the system simple, users "used to" the use of the system. This constant and persistent use of the TWIC card and reader forces the system to be maintained in good operating order. Use in this fashion does not change the operations for the use of the TWIC card and reader from one day to the next, in essence making the use of the TWIC card and reader a "routine" security measure, therefore heightening the probability of detecting an anomalous behavior or TWIC card. For the maritime worker who may visit multiple facilities in a given area, or even up and down a coast, this presents a consistent methodology of use.

There may also be some value to suspending TWIC cards if not used within a certain time period. If a card is not used within perhaps a 120 day time frame, it may indicate that the card is lost or stolen, or perhaps in use by a person who does not have a good and legitimate use for the TWIC card. The other

consideration is of course for mariners who may not call on a TWIC enabled facility for more than 120 days due to being at sea. Initiating some form of auto suspension of the TWIC credential prior to the expiration date is advisable.

- 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?

It is recommended that the “hot-list” be updated electronically to the TWIC readers at least once every 24 hours for MTSA regulated facilities where TWIC cards and readers are required. Electronic updates of the hot list should be passed to the readers directly via a secure methodology that does not require intervention of the facility operator. This methodology of updating the TWIC readers would ensure that the readers are up to date if the facility has days that there is no staff present to update the data.

If the card readers are not updated frequently, the possibility of detecting a lost or stolen card being used inappropriately is not feasible. Likewise, if a TWIC card holder is for some reason invalidated, without a frequent distribution of the hot list, the person may still be admitted to a facility requiring a valid TWIC card for entry.

While a global update to all TWIC readers and facilities with the hot list at least every 24 hours may be appropriate, if a schema could be developed for an electronic push out to facilities and TWIC readers as soon as the TSA determines a card is no longer valid (theft, loss, adjudication) would be preferable.

It is highly recommended that the updates of the hot list to facilities not be done solely by fax or mail, as this has a greater potential to introduce human error on the part of the personnel operating the security systems at the facilities. Likewise, it is imperative that security personnel are not required to scan through a printed list of personnel when checking for people on a “hot list” of invalid cards, as: A) the potential for error is great, and B) this would introduce a significant time delay in resolving a potential problem.

One other concern to be addressed, is how the hot list is to be transmitted, namely are only the most recent updates of “hot listed” personnel distributed, or is a comprehensive list transmitted. It is recommended that a comprehensive list be transmitted to ensure no data is lost or inadvertently over written. Once a hot listed person’s TWIC card reaches its expiration date (expired card) then that individual’s card should be withdrawn from the hot list, as it is by default no longer a valid TWIC card.

Finally, there needs to be a very rapid system by which TSA can be contacted by a vessel or facility to resolve potential conflicts with a hot listed TWIC card. For

example if a “hot listed TWIC card” is reinstated, but the download of data has not reached the facility, this must be able to be resolved quickly by TSA via telephone or other means.

- 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 primary interface where a TWIC card reader would be used by the vessel is at either A) the interaction with the Pilot or B) at the interface and interaction with a facility. With these operational considerations in mind, it is recommended that the updating of the TWIC data for vessels be coordinated through the Pilot for at sea operations. When the vessel arrives at a facility, it is highly likely that the vessel will have an interaction with the Facility Security Officer (FSO) or representative of the facility before any other personnel are authorized for embark/disembark in order to complete the Coast Guard required Declaration Of Security (DOS). At this time and interface, it may be possible for the FSO to temporarily provide an updated mobile TWIC card reader for the vessel's use. Alternatively, the vessel could coordinate with their agent, for the agent to provide an updated mobile TWIC reader for the vessel to use while at the facility.

While the updated hot list may be faxed or otherwise transmitted to the ship without an internet connection, the introduction of error with this methodology could be significant, particularly when the miss-reading of one number or character could adversely impact a valid TWIC card holder. Therefore, this methodology of using a fax to update a hot list is not recommended. Likewise, as the number of “hot listed” persons grows over time, the faxed list would eventually grow to unmanageable proportions for transmission via fax.

- 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?

It is recommended that the use of Digital Signature Checks should be present in every TWIC card to TWIC card reader transaction. The use of a contactless electronic verification of the TWIC card by a TWIC card reader (validation of contents of data on the card, integrity of data on card) and the use of biometrics for all security levels as a minimum standard. This eliminates confusion, as there is one methodology to be used at all times. The Port of Seattle recommends the PIN number not be used as PIN numbers have a very high probability of being compromised, written on the card, or forgotten by the card holder, necessitating contact with TSA which induces delay into the validation process and adversely impacts facility operations.

This said, it is however important to have a methodology to account for the population of TWIC card holders who are not able to enroll a biometric within the TWIC system, as the Port of Seattle has experienced approximately 2% of the population who are not able to enroll their biometrics into our existing fingerprint based biometric capture system. Alternatively, a different fingerprint biometric capture device/technology not based on photographic capture of the surface epidermis fingerprint (photographic, capacitive, inductive, frustrated holographic image, etc.) may resolve this problem.

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.

There is a concern that a schema such as this places the vessel or facility operator at a disadvantage of having to contact the TSA directly for updates of information, potentially on every TWIC card holder accessing the facility, which could number in the thousands.

Alternatively, all facilities that employ TWIC readers could be required to register with the Coast Guard (who already regulate MTSA facilities and vessels that will require the implementation of TWIC) and provide an electronic means of updating the TWIC readers. The TSA should coordinate closely with the Coast Guard so that the facility and vessel operators have one consistent agency with which to interface for TWIC and associated security regulations. With this cooperation in place, the TSA would have a list of TWIC readers to send (push) updated data out to, instead of each individual facility and vessel having to request data (pull).

- 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.

The danger in requiring the owner/operator to be responsible for ensuring the validity of the most recent hot list places the facility or

vessel in a precarious position of responsibility if TSA is unable to deliver the requested updates.

The update of the hotlist data should be on a common schema across the maritime environment, providing consistency of the date and time of automated download of data from TSA. The TWIC readers should have the ability to automatically and autonomously poll TSA directly and synchronize data and the hot list without facility/vessel direct interaction. The TWIC readers should have some mechanism to alert the facility/vessel operator that the data is current and up to date, and provide some sort of alerting mechanism or alarm if the most recent data is not up to date in accordance to the schedule, thus prompting positive action on behalf of the facility/vessel operator.

- 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.

It is recommended that a manual check of the hot list be the last option for resolution of the validity of a TWIC card. This introduces several weak points within the security of the TWIC system. A chief vulnerability introduced by this methodology is the ability of the front line security guard to be sure they have the most up to date printed list to check against, instead of the list that was printed out some time in the past. Likewise checking against a printed list manually introduces a significant probability of human error in missing the name or CHUID of an individual that should be denied access to a MTSA regulated facility or vessel. This system also introduces the possibility of the introduction of a counterfeit or altered hot list, and the potential of social engineering to defeat the system.

If there is any question on the validity of a TWIC card, it should be able to be vetted by a national clearing house toll free telephone call center or the local Coast Guard office. This type of call center would have to be available 24 hours a day, every day of the year, and sufficiently staffed as to avoid lengthy delays in answering the call for validation.

One key element missing in this system is what is the facility/vessel operator or security staff to do with a hot listed TWIC card once it is validated that it is no longer valid? Is there any requirement to alert TSA or the Coast Guard that an invalid card has been attempted to be used? This needs to be clarified.

This system as proposed is very risky and could lead to someone bypassing the system or Socially Engineering their access to an area that they should not gain access to.

Having a 1-800-Number for the inspector to call, provide the badge name, number. This would be a location manned by USCG that could look at the most up to date list may be a viable alternative.

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?

It is recommended that an exemption to the requirement to maintain records be granted for emergency personnel responding to an emergency, i.e. Police, Fire and Emergency Medical personnel. Likewise, record keeping for Coast Guard and other authorized Federal Employees (CPB, ICE, etc.) should not be required.

- 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?

While the concept of keeping records does not in itself raise an objection, there needs to be clarification as to how, and how long the records are to be maintained, and an allowance for human error that is without doubt going to occur. This again points to the necessity of an electronic system that removes to the greatest extent possible the human factor that induces error.

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

It is recommended that the facility be allowed to provide a temporary badge to the individual that expires in 8 hours (max) upon issue.

Require that the TWIC-badged person escorting the individual have their badge expire if the escortee loses their badge or gets separated from the escort – this could be done when the TWIC-badged person leaves the secure area.

Fine the escortee and escorter should separation occur. Penalize the TWIC card holder and the escortee, not necessarily the facility or vessel..

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?

Have the TWIC card checked upon entry to the secure area. Then, when the individual goes aboard the ship, have them use the TWIC Card reader at the gangway to “sign out” of the secure area and onto the ship. Then, when the individual comes off the ship they need to re-badge into the secure area.

- 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?

I agree with the second question – each regulated entity is responsible for validating TWIC’s prior to granting unescorted access to its own secure area.

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?

To make the regulations consistent, and to remove the potential for a person who poses a security risk to the regulated vessel or facility, the individuals should also be required to meet the same TWIC requirements as the vessel or facility.