

MERCHANT MARINE PERSONNEL ADVISORY COMMITTEE (MERPAC)
TASK STATEMENT 67

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. MERPAC'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.

Mr. Andrew McGovern
Chairman
MERPAC

Mark C. Gould
Assistant Executive Director
MERPAC

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:

No drafting of this TWIC 2 NPRM should take place before the pilot reader program is completed and the information tallied and analyzed, as required in the Safe Port Act.

It is essential that the agencies use some facts and statistics, the initial comments of the advisory committees should be incorporated to develop the pilot projects. Undue financial burden has already been placed on this industry, and the additional requirement of mandatory readers proposed in this document would place additional cost on this industry without significant risk reduction for most of the regulated vessels and facilities. Undue burden has been placed on the individuals that work in the US maritime industry. Coast Guard needs to consider, in addition to the information from the Pilot Project, the agency should look at other similar rules within DHS, such as the Chemical Facility Access Rule where risk has been used, setting a performance based standard in a non-

prescriptive manner. Additionally, the International Standard (ICAO) needs to be considered. The background checks and the employers' requirements to make sure all persons accessing secure areas should sufficiently address the security concerns. The proposed requirements of TWIC 2 do not appear to recognize the risk reduction that is gained by conducting the background checks, and then limiting access to those that have been checked.

If there are persons holding TWIC cards that the Government truly believes present a risk and a threat, it should be the government's job to notify industry and take the appropriate action. The government should not try to place the burden of the law enforcement function on the employers of American waterfront operations.

TSA and USCG should not produce another NPRM that is hastily cobbled together, and ignores the input of industry. While the agencies now refer to the over 1900 comments as if that large number is a compliment, they neglect to point out that all but a few were extremely negative about the proposal. It is critical that the agencies wait for the pilot program, to demonstrate to industry that the next NPRM has significantly considered real-world scenarios and application.

- 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?

Readers only increase security in operations that are large enough that facial recognition by each employee does not occur. A reader does not increase security in a small group that would identify a new person immediately, based on facial recognition. One does not need a reader in an office to know that the co-workers today are the same co-workers as last Friday. Validation can be accomplished via a CHIUD list, and for certain operations, that is all that will ever be needed, vessel or facility.

Any vessel or facility that is not regulated by MTSA should not require a reader, regardless of the number of TWIC holders that work on the vessels or facility.

If there is a determination that a reader is appropriate on a MTSA-regulated vessel or facility, because it is the best way to address the risk, the crew size should not be the determination; it should be the risk assessment and the vessel operation that determines the placement of the reader. Whether on the vessel or in the facility that the vessel works with, the goal should be the verification of the cards. Where this is accomplished should be stated in the approved security plan and the assessment should determine the placement.

Should Coast Guard determine that crew size is an appropriate threshold, only vessels with crew members of 100 or more should be required to utilize TWIC readers. The crew size should not consider persons in addition to the crew, only minimum required crew as defined in NVIC 03-07. It should be stated that although marine crew may have TWIC cards, a vessel that is not regulated by MTSA should have a reader, ever.

The Committee suggests that CG keep in mind the fact that the significant majority – as many as 95% -- of the cargo ships calling U.S. ports are foreign flagged, and that these vessels would not be required to incorporate the use of TWIC readers. DHS should be mindful of the fact that it would be inappropriate to implement measures that will disadvantage vessel/cargo processing for U.S.-flagged ships.

Only a pilot test can determine at what size staff you can say that you will always recognize that a new person has been introduced. The NPRM should not be drafted until substantial information is received from the Pilot Program.

- 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).

Some of these factors would be: if the crew are all day workers, if the vessel arrives back at the same facility at least once every 48 hours, if the vessel and facility operate under a combined security plan.

The Pilot Program should address real scenarios of multiple vessel operations during the testing phase, and incorporate those findings into the draft rule. The ability of the personnel to use the reader during real-world work day tasks, and an assessment that an appropriate increase in security has been reached as compared to the cost of the reader and its supporting infrastructure. The costs must include loss of employee productivity if readers create a barrier to task completion.

- 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?

The question presumes that a reader will be standard, and that the exception would be to not having a reader. The committee believes that many vessels and operations will be justified in not having a reader.

This question presumes that crew size is a determination, and this committee feels that crew size may not be a determining factor. More important should be if the vessel owner’s VSP or ASP includes alternative procedures for access control appropriate to the vessel’s size, vessel type, operations, and risk profile; or, the vessel owner enters into an arrangement with the owner(s) of facilities served by the vessel, or also controls the

facility, to use card readers installed at the dock or other appropriate shoreside location. If no location on board can offer a secure installation or the installation would be unreasonably expensive, those considerations should be considered. An example might be no interior space out of the weather. Verification of card by other means (hot list) should be an alternative for a reader.

- 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 goal should be the ongoing verification of the cards. How and where the verification takes place should be determined by the risk assessment of the vessel/facility owner/operator. Coast Guard has already determined that inspections will be done using portable readers to check card validity. Whether a facility chooses to use a TWIC card for an electronic access control system should be the option of the owner/operator.

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

Yes, if a reader is necessary. Vessels often crew up from one central location; a list of invalidated cards should be available to all operations to alleviate the need for readers.

This would allow for the validation of visitors to the vessel/facility that may present a TWIC for unescorted access as well. This validation could be accomplished by a reader OR via a computer database OR printed hot list.

- 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?

Using the results of the pilot program, the Coast Guard/TSA should seek further industry and advisory committee input to determine realistic parameters for type and frequency of checks.

- New Hire – Upon the hire of a new employee the validity of the card should be checked. An online or telephonic system should be sufficient.
- Change in MARSEC Level – A change in a MARSEC level could indicate either a threat against the nation or a threat against the vessel. This would be a reasonable time to recheck the validity of cards. An online or telephonic system should be developed to allow a company to validate without a reader.

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?

DHS should strive for an adequate level of security that also facilitates commerce and supports the rights of mariners. To that end, the check of one security element that proves the card is valid and one element which proves the holder is the registrant should suffice at any MARSEC level.

The available features should only give flexibility to those that install card readers, and provide backup when the primary technology fails, or when security personnel have reason to believe that the card presented has been altered.

Of the 5 choices above, the last choice for workers should be the use of the PIN, since the PIN will not be used frequently enough to remember without a written record.

Vessels/facilities should be able to determine whether TWIC readers should be used at all based on their level of risk. At some low-risk vessels/facilities, using a TWIC as a flash pass should be sufficient. The access control system used by the vessels/facilities would be incorporated into the security plan and approved by the Coast Guard.

The CSO/FSO for each vessels/facility should determine how frequently they need to update the hot list. Risk should be used to determine the frequency of that check. This should not be required until TSA has demonstrated that its system is fully automated and compatible with most legacy access control systems. In addition, the frequency with which a vessel/facility must update the hot list can only be determined after TSA provides information on how often the database will be updated.

- 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?

Yes, it should be based on risk. The regulation should not attempt to dictate what individual vessels/facilities do or how frequently, but allow sufficient flexibility through the security plan process, just as is done currently. Even at higher MARSEC levels, not all vessels/facilities will need to validate with the same frequency; a 24/7 operation might require more frequent updates than one which is often idle. Seasonal operations will not (should not) be checking card validity during non-operational months. Information from Pilot Program will be essential in answering this question, and the drafting of this language should be delayed until such pilot program information is available.

TSA needs to describe the system that it will use to update criminal background, mental health or security threat information on card holders. If the information is not being continuously updated by the government, then what would be the purpose of checking card validity constantly?

- 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?

MARSEC Level and other comments as above. 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 verification system is only as effective as the most recent data available. During the pilot program, information should be found about the realistic updating of the information on the 'hot list' by TSA.

- 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 approved VSP/ASP/FSP should establish a minimum frequency, based on risk and 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, if the Coast Guard does require that TWICs be verified against the hot list periodically at MARSEC 1, a vessel owner's VSP or ASP could specify that it is the responsibility of the Company Security Officer to ensure that the invalidated 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 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 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.

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).

However, if option a) is put in place, then the employer should not be required to also complete b) and c).

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

Owner/operator/labor suppliers should be provided the flexibility of uploading/downloading multiple employees "identifier" allowing automated query of the TSA "Hot List" database. This would allow large marine and labor employers the ability to vet thousands of records at one time. Standards for the format, transfer and reconciliation of this data will be discussed with owner/operator/labor prior to publishing a final rule.

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, as well as the requirements of vessel and facility operations. Log books, time cards, payroll records; all provide sufficient information to TSA.

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 the access to restricted and secure space is adequately addressed under existing vessel and facility operations and see no need for requirements in this regard for additional recordkeeping. Large facilities and facilities with a high risk, such as tank farms, LNG facilities, etc. should address risk in their plans. The rule should not attempt to address these high risk, large facilities in a manner that would be overly burdensome for small operations with vessels with small crews, such as towing vessels.

The individuals that are granted unescorted access are those that have had a background check, and proven that they are not terrorists. They should not have to then prove it again every time they need to check a valve temperature in the engine room! Tracking every entry into a restricted space is excessive, redundant and will impede the commerce of that vessel unnecessarily with no shown risk reduction.

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

None. 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, and business documents.

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?

This should be an option for certain facilities that have an appropriate working relationship with a vessel. A card reader may not be necessary. The determination of whether to purchase a card reader, and then select the location of those 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 may 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.

The Coast Guard should retain the concept introduced in the May 22, 2006 proposed rule, which introduced the concept of “recurring unescorted access”. Defined as the authorization to enter a vessel on a continual basis after an initial personal identity and credential verification, as outlined in the vessel security plan. Essential for these operations, TWIC verification should only be required once, to assure that the employee has the required credential, and then reoccurring access should be allowed, both for the facility AND the vessel. This is essential for the facilitation of these operations.

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?

If the facility is owned and operated by the same entity, then it is a joint obligation, and there should be no requirement for a DoS. Vessel and facility owners should be allowed to work together to arrive at mutually acceptable arrangements that can be documented in the appropriate security plan. Use of a DoS is already spelled out in those plans, and while TWIC procedures will be added to the plan, and DoS may have to be modified, the DoS requirements will not change. .

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?

As for the issue of “state pilots” there are no state pilots without CG credentials and on a practical manner a pilot will not be able to work without a TWIC due to access issues. This is a non issue and there are more important issues to deal with.

The Coast Guard should issue a notice of proposed rulemaking requiring all personnel serving as a pilot and 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.

Additional Recommendations:

U.S, flag vessels in foreign service should be exempted from TWIC requirements while operating in a foreign port, since port workers would not hold TWIC cards.. This exemption should be similar to the exemption already given to offshore supply vessels.

We concur and reiterate the closing position of TSAC:

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.