The American Waterways Operators
www.americanwaterways.com

801 North Quincy Street
Suite 200
Arlington, VA 22203

PHONE: (703) 841-9300
Fax: 703) 841-0389
E-MAIL: jcarpenter@vesselalliance.com

Jennifer Carpenter
Senior Vice President - National Advocacy

May 26, 2009

Docket Management Facility (M-30)
U.S. Department of Transportation
Room W12-140
1200 New Jersey Avenue, S.E.
Washington, D.C. 20590-0001

Re: Transportation Worker Identification Credential (TWIC) – Reader Requirements (USCG-2007-28915)

Dear Sir or Madam,

The American Waterways Operators is the national trade association for the tugboat, towboat, and barge industry. AWO's members account for approximately 80 percent of the barge tonnage and two-thirds of the towing vessel horsepower in this critical industry segment, moving cargoes essential to the American economy on the inland rivers, the Atlantic, Pacific, and Gulf coasts, and the Great Lakes. Tugboats also provide essential services, including shipdocking, tanker escort, and bunkering, in ports and harbors around the country. On behalf of AWO's members, thank you for the opportunity to comment on the advance notice of proposed rulemaking (ANPRM) outlining the Coast Guard's preliminary thinking on the development of the Transportation Worker Identification Credential (TWIC) card reader requirements.

We submit these comments from the perspective of an industry that is serious about security. Immediately after September 11, 2001, we began working with the Coast Guard and the U.S. Army Corps of Engineers to develop a Model Vessel Security Plan for towing vessels, more than a year before such plans were required by law. When the Maritime Transportation Security Act (MTSA) was enacted in November 2002, AWO worked with the Coast Guard to transform the Model Vessel Security Plan into one of the first Coast Guard-approved Alternative Security Programs. AWO members work hard to transport our nation's cargo safely and securely, and we take pride in the fact that our American-owned, American-crewed, American-built vessels are the "eyes and ears on the waterways" for the Coast Guard.

AWO commends the Coast Guard for publishing an ANPRM as the first step in this rulemaking process. The card reader issue has been deeply controversial since proposed reader requirements were first included in the May 2006 notice of proposed rulemaking (NPRM) for the TWIC program. AWO was a strong supporter of the August 2006 decision by the Coast Guard and the Transportation Security Administration (TSA) to separate the reader issue from the rest of the TWIC rulemaking and reconsider it in a fresh light. Beginning this process with an ANPRM rather than proceeding directly to an NPRM sends a welcome signal that the Coast Guard recognizes the complexity of this issue and intends to proceed thoughtfully and deliberately.

AWO also appreciates the Coast Guard's attempt to take a risk-based approach to the establishment of TWIC reader requirements and its recognition that electronic card readers add little or no security value in some circumstances, such as on vessels with limited crew sizes. We approach this rulemaking from the same philosophical perspective. However, we take a different view of how the concepts of risk and value-added should be applied in deciding whether and where electronic card readers should be required. The comments that follow elaborate on the intellectual framework that we believe should guide the development of card reader requirements and propose a different approach to the establishment of reader requirements on vessels. Our approach is driven by the following premises:

1. The use of card readers on vessels is not required by Congress. The Coast Guard could fully implement its obligations under MTSA and the SAFE Port Act without requiring electronic card readers to be used on vessels or by vessel owners.

2. A risk-based approach to the card reader question should take into account all of the risk-reduction measures that have been implemented pursuant to MTSA and the SAFE Port Act and should consider the incremental value to be gained through a card reader requirement.

3. The requirement for certain personnel to obtain a TWIC has added significant security benefits that exist independently of the use of card readers.

4. Operational factors (e.g., crew size, number of individuals attempting to gain access at one time, etc.) are highly relevant in determining the value of a TWIC reader in a given circumstance.

We elaborate on these premises below.

An Intellectual Framework for the Consideration of TWIC Reader Requirements

The Use of Card Readers on Vessels is Not Required by Congress

We note, first, that the Coast Guard is under no Congressional mandate to establish reader requirements for any class of vessels. Section 70105 of MTSA 2002 requires the issuance of a biometric transportation security card to enumerated categories of individuals and requires the issuance of regulations to prevent an individual from entering a secure area of a MTSA-regulated vessel or facility unless that individual is authorized to do so and either holds a transportation security card or is accompanied by another individual who does so. The act neither makes nor implies a requirement for electronic card readers.

Four years later, in the SAFE Port Act, Congress responded to significant public concern about a potential requirement for card readers (as reflected in numerous comments to the docket on the May 2006 TWIC NPRM), especially on vessels with limited crew sizes. The SAFE Port Act provides that the Coast Guard may not require the placement of a card reader on a vessel unless the vessel has more than the number of TWIC-holding individuals in its crew that the agency determines warrants the use of a reader, or unless the Coast Guard determines that the vessel is at risk of a severe transportation security incident. The operative phrase is "may not." Not only did Congress not mandate that the Coast Guard establish card reader requirements for any class of vessels, but it explicitly precluded the establishment of reader requirements for vessels that do not meet these statutory criteria. Within these statutory parameters, the Coast Guard may – or may not – elect to establish reader requirements on vessels. We urge the Coast Guard to bear this discretion in mind.

A Risk-Based Approach Must Consider Potential Reader Requirements in a Broader Context

As stated above, AWO respects and supports the Coast Guard's attempt to take a risk-based approach to the establishment of TWIC reader requirements. However, we believe that to be most meaningful, the Coast Guard's risk assessment should take into account all of the risk-reduction measures that have been implemented pursuant to MTSA and the SAFE Port Act and should consider the incremental value to be gained by establishing a card reader requirement for a particular class of vessels or facilities. By contrast, the approach outlined in the ANPRM seems to consider the card reader question in a vacuum. The Coast Guard first categorizes vessels and facilities into three "risk groups" and then proposes a complex set of reader requirements for those in the two higher risk categories.[1]

[1] Later, the Coast Guard introduces the concept of "recurring unescorted access," which allows up to 14 individuals at a time to be granted access without the use of card readers at each entry.

We believe this approach misses the mark for two reasons. First, we question the need to establish new risk groupings for vessels when risk has already been taken into account in applying the MTSA 2002 vessel security plan requirements and the TWIC requirements themselves. In other words, Congress and the Coast Guard have already determined that certain vessels pose a higher risk of a transportation security incident and are therefore required to have Coast Guard-approved security plans. The Coast Guard has taken risk into account in approving security plans for these vessels, ensuring that more stringent risk-reduction measures are implemented when a vessel is carrying certain dangerous cargo (CDC) or operating at a higher MARSEC level. TSA and the Coast Guard have taken this concept even further with the implementation of the TWIC requirements, which have now been incorporated into vessel security plans. Against this backdrop, we find it unnecessary – and unnecessarily complex – to further divide vessels into risk groups for the purpose of applying TWIC reader requirements.

Our second concern with the Coast Guard's proposed approach is that it seems not to focus on the critical question of the incremental risk-reduction value that a TWIC reader would add in a particular circumstance (although the Coast Guard later hints at this concept through the recurring unescorted access provision). Vessels with Coast Guard-approved security plans (including towing vessels and barges using the AWO Alternative Security Program) are already subject to an extensive array of risk-based security measures, including, but not limited to, requirements for personnel training, drills and exercises, security communications, and access control, as well as special provisions for restricted areas, monitoring, cargo handling, and delivery of stores and supplies. As of April 15, 2009, such vessels are now subject to a higher level of risk reduction, as only authorized personnel who have successfully completed the rigorous security threat assessment required to obtain a TWIC can be granted unescorted access to secure areas. The key question to be answered in this rulemaking is, "Are there some vessels within this universe for which use of a card reader adds material security value <u>on top of the security measures that are already in place</u>?"

The TWIC Requirement is a Significant Risk-Reduction Measure with or without Card Readers

To answer this question, we believe it is important, first, to note that implementation of the TWIC requirement is a significant risk-reduction measure, independent of a potential requirement for card readers. As of April 15, 2009, anyone seeking unescorted access to a secure area of a vessel or facility covered by the MTSA 2002 security plan requirements must have passed a stringent TSA-administered security threat assessment. TWIC enrollment procedures, which include fingerprinting and the presentation of two identity documents, ensure that it will be extremely difficult, if not impossible, for an individual to obtain a TWIC fraudulently. And, the incorporation of the TWIC requirements into vessel and facility security plans means that vessel and facility personnel are trained to ensure that only TWIC-carrying or appropriately escorted personnel obtain access to secure areas. An electronic card reader is not required to achieve these very real security benefits.

In our view, the potential value of a card reader is twofold: first, using a reader may provide a more reliable means (as compared to visual inspection) of verifying that the holder of a TWIC is, in fact, the person to whom the TWIC has been issued under some circumstances. The second potential benefit of a card reader is providing a means to determine whether a validly issued card has become invalid for some reason. The degree to which a card reader actually provides value in these two respects will be influenced by the nature of the vessel (or facility) operations in question, as well as other measures in place to guard against these two security risks.

Operational Factors are Important in Determining the Value of a Card Reader in a Given Circumstance

Whether use of a card reader is a material improvement over visual inspection to verify that the holder of a TWIC is the person to whom the card has been issued will depend in large part on two factors: the extent to which the holder of the card is known to the person inspecting the card, and the number of personnel who will be attempting to gain access to the vessel or facility at any given time. For example, it may be difficult for a guard at a busy port facility with hundreds of workers entering a single gate at shift change to take the time to scrutinize each worker's TWIC carefully. A TWIC reader may have value in this circumstance. By contrast, on most vessels, with the possible exception of large cruise ships, the number of personnel attempting to board the vessel at any given time will be very limited. Vessel personnel will have ample opportunity to scrutinize the TWIC of anyone seeking unescorted access (and even, in case of question, contact the company office for further guidance). If, as in the case of most towing vessels, crews are well known to each other, an electronic card reader would add even less value.

Whether use of a card reader is needed to ensure that a validly issued card has not been rendered invalid for some reason depends on the other options available to verify the validity of a card. The most likely reason that a card will no longer be valid – it has expired – can be easily checked during a visual inspection. Again, the ability to conduct a thorough visual inspection, including a check of the card expiration date, is enhanced when the number of individuals seeking access at any given time is limited. A card might also become invalid if it has been reported lost or stolen, or if the holder commits an offense that places him or her on the TSA Hotlist. While a card reader is one way to check whether a TWIC has been placed on the Hotlist, there are other practical options, including the system of "privilege granting" discussed in the ANPRM or a Web-based system (perhaps using Homeport) in which an employer runs a check of employees' TWIC numbers against the Hotlist.

The presence of card readers elsewhere in the transportation system is also a factor that influences the value-added of card readers on vessels (or in the offices of vessel owners). It is likely, for example, that many facilities through which vessel personnel will pass will have card readers installed (either because they are required by regulation or because the facility owner chooses to do so). In addition, the Coast Guard has made clear public

statements that it intends to use handheld card readers to conduct TWIC validity checks in the course of its maritime security activities. This means that vessel crewmembers' TWICs are likely to be checked with readers on a routine basis even if card readers are not required on vessels and vessel owners are not required to use card readers, further diminishing the risk-reduction value of a reader requirement for vessels.

TWIC Reader Requirements: AWO's Proposed Alternative

Considering these premises together, AWO recommends a simple, straightforward approach to the establishment of TWIC reader requirements for vessels: eliminate the "recurring unescorted access" provision and provide that vessels with fewer than 14 required crew members will not be required to carry a card reader; eliminate the risk group concept for vessels and require a thorough visual inspection of the TWIC when a new crewmember is hired, when a crewmember boards the vessel at the beginning of his or her tour of duty, and when any other individual seeks unescorted access to the vessel; and, establish a privilege-granting system in which TSA notifies employers when an employee's card has been placed on the Hotlist. We elaborate on the components of this recommendation, as well as other questions posed by the Coast Guard in the ANPRM, below.

First, AWO strongly supports the Coast Guard's recognition that card readers add no security value on vessels with limited crew sizes. The proposal not to require card readers on vessels with fewer than 14 crewmembers is consistent both with the intent of Congress as manifested in the SAFE Port Act and with the advice of respected federal advisory committees such as the Towing Safety Advisory Committee (TSAC). Consistent with the intellectual framework outlined above, however, we recommend that the Coast Guard take a simpler and more straightforward approach to accomplishing this end than the "recurring unescorted access" provision discussed in the ANPRM. Instead, the forthcoming NPRM should simply state that card readers will not be required on vessels with fewer than 14 required crewmembers. On a vessel of this size, crewmembers are generally known to each other and there are never more than a small number of individuals (crewmembers or authorized non-crewmembers) attempting to gain access to the vessel at any given time. A card reader is not necessary in these circumstances.

Second, we urge the Coast Guard not to tie reader requirements to the proposed risk groups. As discussed above, we believe categorizing vessels by risk group is unnecessary given the risk-based approach that is already reflected in the application of the MTSA 2002 vessel security plan requirements and the proposal not to require card readers on vessels with limited crew sizes. We also have serious concerns about the practicality of applying reader requirements to vessels based on risk group. Under the risk group structure, it will be common for towing vessels to move back and forth between risk groups – from A to C and back again -- depending on the cargo of the barge in tow. The proposed requirements do not seem to take this operational reality into account. For example, how does a vessel with fewer than 14 crewmembers that is in risk group C today and risk group B tomorrow comply with the requirement to conduct periodic card validity

checks? When the vessel is in risk group C, a monthly check of the expiration date is required. When the vessel is in risk group B, a weekly electronic check of the card against the TSA Hotlist is required. We urge the Coast Guard to abandon the risk group concept as it applies to vessels.

Third, we urge the Coast Guard to eliminate the requirement that vessel owners use a card reader to conduct an initial biometric match of a new employee's TWIC. It is redundant to impose this requirement on vessel owners when the same match has already been conducted by TSA at the time of card activation. Instead, vessel owners should be required to conduct a thorough visual inspection of the TWIC when a crewmember requiring a TWIC is hired, when he or she boards the vessel at the beginning of his or her tour of duty, and when an authorized TWIC-carrying non-employee seeks unescorted access to the vessel. As discussed above, a visual inspection of the TWIC to ensure that the bearer is the person whose photograph (biometric) is on the card is a legitimate and practical way to conduct a biometric match when circumstances allow for a careful examination. The Coast Guard has issued detailed guidance to vessel and facility security officers and local law enforcement regarding visual inspections and we urge the agency to utilize the expertise of these partners in the TWIC implementation process. Under the less burdensome approach we are proposing, vessel owners would no longer be required to purchase a shoreside card reader, but crewmembers' TWICs would still be run through card readers on a regular basis at facilities and by Coast Guard field personnel, allowing for a full biometric check using the TWIC security features to supplement visual inspections by vessel owners.

Fourth, AWO supports the creation of a "privilege granting" system in which TSA alerts vessel or facility owners when an employee with unescorted access to secure areas has been placed on the TWIC Hotlist. This is a better alternative to the proposed requirement that owners of vessels in risk groups A and B check the continued validity of employees' TWICs on a weekly or daily basis, depending on the MARSEC level. It would also solve the problem of figuring out how to meet the card validity check requirements when a vessel operates in different risk groups from day to day. We recommend that privilege granting be the standard mechanism for allowing employers to ensure the continued validity of employees' TWICs; there should be no fee to provide TSA with a list of employees' TWIC numbers and receive notification from the agency if and when an employee's card is placed on the Hotlist. The Coast Guard and TSA should also consider other practical means of allowing employers to check the continued validity of an employee's TWIC, such as a web-based searchable version of the Hotlist, which could be made accessible to authorized persons on Homeport. An employer who wishes to verify that an employee's TWIC is not on the Hotlist should have a means to do so on a real-time basis.

We also wish to comment briefly on several other issues on which the Coast Guard has requested comment:

- **PIN use:** AWO strongly supports the Coast Guard's proposal not to require use of the TWIC Personal Identification Number, or PIN, as a means of TWIC holder verification at any MARSEC level. Requiring a PIN is unnecessary from a security standpoint and will likely result in significant disruptions to the efficiency of maritime commerce. AWO urges the Coast Guard not to reconsider its decision against use of the PIN, and AWO encourages the Coast Guard and TSA to continue to communicate to facility owners that the agencies do not expect facilities to require use of the PIN, either.

- **Recordkeeping:** AWO urges the Coast Guard to avoid overly prescriptive recordkeeping requirements. AWO does not object to the proposed requirement that companies maintain records for two years of employees granted unescorted access to secure areas, as employee information is already maintained in human resources and payroll records. However, the Coast Guard should not prescribe the method in which these records are kept, nor should the agency require the routine submittal of such information. Rather, employers should only be required to share such information with the Coast Guard upon request in the case of a legitimate need to know (for example, a law enforcement situation).

- **Inspection of TWIC readers:** AWO urges the Coast Guard not to establish third-party or Coast Guard inspection requirements for card readers. As noted in the ANPRM, existing regulations already require that security equipment (including card readers, if they are present) be inspected, maintained, and calibrated according to manufacturer's recommendations. Records of such inspection and maintenance would be subject to audit as part of a company's safety management system.

- **Security plan amendments:** AWO does not object to the Coast Guard's proposal to require amendments to vessel security plans or Alternative Security Programs to address the card reader and associated requirements within six months of publication of a final rule. However, the Coast Guard should ensure that it has built in a reasonable time frame to allow vessel owners to come into compliance with their security plan or ASP after it is approved by the Coast Guard. When the AWO ASP was amended this year to include the TWIC requirements, for example, the plan was approved by the Coast Guard less than two weeks before the April 15, 2009 deadline by which vessel owners were expected to be in compliance with the plan (despite the fact that it had been submitted for approval more than three months earlier). AWO urges the Coast Guard to safeguard against this situation in establishing deadlines and procedures for plan amendment and review in the eventual final rule.

###

Thank you for the opportunity to comment. AWO stands ready to assist the Coast Guard in developing a simpler and more straightforward approach to this rulemaking that ensures high standards of maritime security and avoids unnecessary expense and disruption to vital maritime commerce. We would be pleased to answer any questions or provide further information to assist the Coast Guard in the development of an NPRM.

Sincerely,

Jennifer A. Carpenter

Jennifer A. Carpenter