



# MARITIME EXCHANGE

for the Delaware River and Bay

*Leading the Way to Port Progress*

John T. Reynolds, Chair  
Uwe Schulz, Vice Chair  
Dennis Rochford, President  
Lisa B. Himber, Vice President  
A. Robert Degen, Esq., Secretary, Solicitor  
James F. Young, Esq., Assistant Secretary  
Dorothy Mather Ix, Treasurer

May 19, 2009

Docket Management Facility  
U.S. Department of Transportation  
Room Plaza W12-140  
1200 New Jersey Avenue, SW  
Washington, DC 20590-0001

**RE: USGC-2007-28915**

This letter is in formal response to the request for comments to the above-referenced Advanced Notice of Proposed Rulemaking (ANPR). The Maritime Exchange for the Delaware River and Bay is a non-profit trade association representing port operators and maritime businesses throughout Southeastern Pennsylvania, Southern New Jersey and Delaware. Exchange members include both regulated facilities and vessels as well as industry members who require access to multiple facilities and vessels.

The discussion below reflects the views of the Maritime Exchange as well as the members of the Sector Delaware Bay Area Maritime Security Committee Port Business Operations Sub-committee.

**Risk Groups:** First, we appreciate the Coast Guard's effort to implement TWIC using a risk-based method rather than a one-size-fits-all approach. We also appreciate the use of MSRAM to derive information that can be used in the day-to-day operation of our nation's maritime and port system. However, it is our understanding that the MSRAM data are several years old at this time and may not reflect current vessel and port security risks.

However, we do not believe the risk groups as outlined in the ANPR reflect the totality of possible scenarios, nor can they be implemented in any practical manner. First, the risk group methodology does not address decreases in risk which facilities may achieve through use of PACS – Physical Access Control Systems – such as the ability to limit access based on date/time only to individuals previously scheduled to work at that date/time. Further the implementation methodology is unclear. For example, is a Risk Group B facility in Tier/Group I port more vulnerable than one in a Tier/Group III port? The risk groups outlined in the ANPR do not account for the risk/threat differences among the nation's seaports.

The means to classify facilities which move between risk levels is not defined. If a facility generally defined as in Risk Group C handles one vessel per month with CDCs, for example, would it be temporarily classed as a Group B facility or must it permanently maintain the higher designation? Similarly, the ANPR does not provide a mechanism for a Group C facility handling a Group B vessel or other situations wherein individuals move between and among risk groups.

Nor does it address such issues as ships' provisions; for example, if a Group C vessel at a Group C facility receives a shipment of paint, does the paint, classified as a hazardous materials, increase the risk?

In short, the effort to classify various scenarios would result in an implementation matrix that is overly complex and difficult to implement. If Coast Guard ultimately elects to maintain this approach, further clarification is needed, and regulations and guidance must be simple to understand, enact and enforce; if not, a great deal of discussion and interpretation will take place between the facility, the USCG Sector and USCG HQ each time a situation arises.

However, given that we support efforts to implement TWIC based on risk, we recommend as an alternative to the pre-defined risk groups that each vessel/facility operator determine its TWIC regimen based on its own operating environment and security needs. Procedures for identity verification (biometric match), card authentication, and card validity check would be included in the vessel/facility security plans. These plans would include processes for worst-case scenario, most probable, etc., and be subject to approval by the Coast Guard through the already planned security plan update program.

**Mandatory Biometric Check:** Although not proposed in the current ANPR, we believe Coast Guard will receive comment from individuals who believe that TWIC is worthless without a 100% biometric check at every access attempt. We strongly disagree. There is value in the individuals undergoing the threat assessment at TWIC enrollment, particularly when keeping in mind that most individuals requesting access to regulated areas are known to security staff. In addition, the 100% biometric check might be deemed only somewhat beneficial unless coupled with an instant hotlist check. Needless to say, such a regimen is not practical when weighed against the potential impact to operations.

Bottom line, the utility of the biometric check must be evaluated against the vessel/facility risk as well as impact to operations. Using fingerprints for regular, daily access will present significant logistical problems in the maritime environment, as no doubt a thorough pilot program will demonstrate.

- Contact readers which will quickly become dirty (from hands, weather, bird droppings, dust, etc).
- Biometric verification will add to the delay that contact readers typically entail, especially in outdoors and bad weather conditions.
- Fingerprints are not all that reliable in a population that works with their hands
- In cases of health concerns (swine flu), people will refuse to touch the contact readers, unless a process (and expense) is added for sanitizing the readers between uses (wipes, disinfectant).
- Facilities will most likely need to spend additional dollars so support backup technology readers, or deactivate access control points when equipment is non-operational both of which are cost-intensive activities.

Finally, there are many reports of TWIC cards physically breaking down over time, where they delaminate, the magnetic stripes demagnetize, and the chips are compromised. The less contact the card needs to make with readers, the better.

**Personal Identification Numbers (PINs):** We agree that a requirement for the use of a PIN would have a negative impact on large scale throughput during access control evolutions. We do not support the requirement to use a PIN for access control at any MARSEC level.

**Recurring Unescorted Access:** We appreciate the Coast Guard's consideration of mechanisms designed to speed access control procedures where possible. However, there is little relevance to the number "14" in terms of facility operation and on many regulated vessels. If the Coast Guard is going to allow this type of access, the number of individuals who may be granted recurring unescorted access should be based on the individual vessel/facility environment and included in the security plan.

**Reader Compliance Checks:** Given the increasing demands on Coast Guard time and resources, we suggest that this is one area where the agency does not need to concern itself. Normal business operations will ensure that vessel/facility operators operate readers in accordance with manufacturer instructions, for example, lest any warranties be invalidated. Similarly, if a reader is not functioning properly, business demands will dictate that the owner/operator ensure its speedy repair and implement backup equipment during its outage if needed. Simply stated, we do not believe adding a "calibration test" or other technical verification to the Coast Guard inspectors' scope of responsibility is necessary.

**Security Plan Updates:** The proposed six-month update time period is reasonable; we support a staggered approach.

**Recordkeeping:** While we understand that having records of individual granted unescorted access may be helpful, it seems that it might be more beneficial from a security perspective to identify those individuals granted access with an escort.

For those facilities where (TWIC or PACS) readers are used, the length of record storage period should be established based on USCG investigation timeframes as storage costs money and space. If USCG only needs 12 months, then use 12 months.

**Hotlist Check:** Connection to on-line "hotlists" needs to be easy, reliable and secure. Further, the ability to check on demand, much like an ATM or credit card, should be provided as an option. In addition, the concept of charging a fee for proactive Hotlist updates does not align with the federal responsibility to provide support to non-federal security enhancement initiatives. This option should be available to owners/operators at no fee.

**Publishing Reader Specifications:** We support the position of the American Association of Port Authorities that the Coast Guard should publish as soon as possible a public list of reader specifications in order to allow facilities, particularly those which have received TWIC reader

Coast Guard Docket USGC-2007-28915

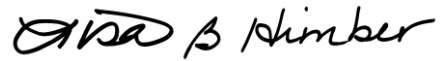
May 19, 2009

Page 4

grants, to evaluate vendors and allow ports to make these security enhancements more quickly and in accordance with the three year limit on grants.

Thank you for the opportunity to comment on this ANPR.

Sincerely,

A handwritten signature in black ink that reads "Lisa B. Himber". The signature is written in a cursive, flowing style.

Lisa B. Himber  
Vice President