



MARITIME EXCHANGE

for the Delaware River and Bay
Leading the Way to Port Progress

Richard E. DeGennaro, Chairman
John T. Reynolds, Vice Chairman
Dennis Rochford, President
Lisa B. Himber, Vice President
A. Robert Degen, Esq., Secretary, Solicitor
James F. Young, Esq., Assistant Secretary
Dorothy Mather Ix, Treasurer

June 16, 2006

Docket Management Facility
U.S. Department of Transportation
Room Plaza 401
400 Seventh Street, SW
Washington, DC 20590-0001

RE: TSA-2006-24191

This document is in formal response to the request for comments to the above-referenced docket. 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. As participants in the East Coast TWIC pilot program, we believe the Exchange and its members are uniquely qualified to comment on this docket.

The discussion below reflects the views of the Maritime Exchange as well as the members of the Delaware River TWIC Stakeholder Working Group.

Please allow us to open by stating two overarching principles which must guide the implementation of the TWIC program: First, it is important to remember that TWIC, as originally envisioned, was planned to serve as a tool to facilitate access to secure maritime vessels and facilities for those with both a legitimate need and the right to obtain such access. The lack of TWIC was never intended to deny access. This was the original concept proposed by USDOT, and later the Transportation Security Administration, and it was because of this vision that industry embraced the TWIC concept.

Second, at all levels within the Congress and the Administration, policy makers have repeatedly stated that it is critical that the United States Government must achieve a balance between security and commerce. Simply stated, if the U.S. economy suffers as a result of onerous and expensive security measures which impede trade, we will not have won the battle against those who would seek to do us harm.

It is with those principles in mind that we offer the following specific comments.

49 CFR

VI. Analysis of TSA Proposed Rule

Waiver Procedures: We support the concept that an individual who knows he or she will not meet the threat assessment standard should have the opportunity to initiate a waiver at the time of

application and recognize that it will be necessary for the individual to pay for the information collection and threat assessment and undergo the full background check.

Scope and Standards for HME Security Threat Assessment: We support the initiative by TSA to identify comparable standards to eliminate the need for individuals who have already successfully completed a security background check to undergo another check for TWIC. Rather than TSA working individually with multiple agencies, DHS should at the departmental level work within its own agencies and those of other departments to establish a federal standard. For example, in addition to an MMD, HME or FAST assessment, many individuals in the armed forces have undergone assessments, as have many AMSC members, or energy sector employees. TSA should not be charged to coordinate these screenings for all individuals simply because they may also need access to regulated maritime areas.

Applicant Responsibilities for a Security Threat Assessment for TWIC: We agree that TSA and Coast Guard should work collectively to implement a staggered rollout for TWIC. We also agree that Area Maritime Security Committees are well positioned to assist the FMSCs in establishing local rollout plans. However, a) since the total initial TWIC population remains unknown (as evidenced by the fact that TSA has asked potential vendors to help identify this number and based on comments in the proposed rule and shared during the public hearings) and b) there remains a significant number of untested processes which will be included in the full program deployment, we believe it is premature to attempt to define a timeline for enrollment beyond the first group. This will be discussed further below.

In addition to enrollment centers at port locations, we suggest TSA establish and staff centers at local USCG Sector Command offices as well as other areas identified by the AMSCs.

The TSA indicates that it anticipates enrollment times will be consistent with normal port operations; it should be noted that the maritime transportation industry operates on a 7-day, 24/7 schedule. TSA should offer night and weekend enrollment options.

Finally, for the last four years, vessels/facilities have been attempting to install access control systems to comply with security mandates. These operators have continuously looked to TSA for guidance on technology standards to be used for TWIC to ensure investments in their systems would not be wasted once TWIC were deployed. Unfortunately, TSA has not been able to provide such guidance – and cannot do so even as of the date of this letter. Accordingly, for those facilities which have recently (within the last zero-three years) installed such systems, we do not believe the TWIC rollout schedule provides sufficient time for them to recover their costs. We therefore suggest that DHS include a mechanism to grandfather these facilities until their expenses have been fully amortized.

SubPart E – TWIC Fees

C. Fee Collection: Since the applicants will be required to provide payment at the application process, TSA must accept cash as many applicants will not have credit cards and others will not have checking accounts. If the final rule does not include a provision for cash payments, we ask that TSA provide the rationale for this decision. We further suggest that TSA include an option to provide credit card information via the web portal.

PREAMBLE

III.B.1. TWIC Process

a. Pre-Enrollment and Enrollment.

Trusted Agents: In addition to the criteria that all enrollment personnel successfully complete a TSA security threat assessment and receive a TWIC before they are authorized to access documents, systems or secure areas, we strongly believe enrollment center personnel should undergo financial history checks as well. An individual in the position to process and issue a TWIC, which will be considered a valuable commodity to someone with terroristic intentions after the program is deployed, should be held to a much higher level of scrutiny. We further believe that all personnel associated with the development and operation, including hardware technicians, programmers, project managers, and others involved in the program should be required to undergo a security screening.

We would like additional information about the training the enrollment center personnel will undergo in the use of the TWIC equipment and how they will be trained to detect fraudulent identity documentation. Finally, we believe that enrollment center personnel must also undergo specific customer service and financial systems management (e.g. credit card readers) training. During the pilot program, there were several individuals employed as trusted agents who presented an unprofessional appearance or demeanor, or more importantly, were unfamiliar with the systems and/or unable to operate the equipment effectively. This led to multiple delays in enrollment processing; TSA should require their or their agent's personnel undergo thorough training well before the program is deployed to minimize the delays once TWIC is implemented.

Lead Time: Since TSA cannot guarantee that any threat assessment will be completed in less than 30 days, there must be a mechanism to allow applicants to access vessels/facilities without escort (should the facility/vessel operator agree to grant it) during the application process.

Enrollment Center Locations: It is clear that a sufficient number and convenient locations of TWIC enrollment centers will be critical to successful program deployment. As of the date of this letter, the location information has been posted on the TSA website, but the specific information (e.g., numbers and locations of readers within those cities) is not yet available for review and comment. We suggest TSA work closely with the regulated public to make the decisions associated with finalizing the enrollment center details.

On-Line Pre-Enrollment: We applaud the use of a web portal to process pre-enrollment information and agree that this feature of the TWIC program will help speed the enrollment process. However, during the TWIC pilot program, the pre-enrollment process was tested using an employer (system administrator) sponsor. Individual applicants were not granted access to use the web portal. We believe TSA should test the individual applicant process to identify and resolve problems prior to formal program deployment.

Document Scan: We question the need to scan and store applicant documentation. Files of this nature require an inordinately large amount of disk storage space, unnecessarily driving up the costs of the program, with out any offsetting security benefit. Further, given the incidence of identity theft today, we believe storing identity documentation only increases the risk that personal data may be compromised.

Biometric Scan: As stated in the preamble, TSA plans to use a digital photograph in situations in which an applicant is unable to provide fingerprints. While this will suffice for card enrollment, it is not clear how it aligns with the vessel/facility requirement to electronically match an individual's biometric with the biometric stored in the card prior to granting access. This should be clarified in the final rulemaking.

Initial Enrollment: As discussed above, it is important that we be provided with more detail on the phase-in approach and that once TSA and Coast Guard provide specific information, there must be an opportunity for the regulated public to comment on and, working with DHS, modify the schedule as necessary.

b. Adjudication of Threat Assessment.

Electronic Communication: To the extent that TSA has developed a secure electronic method of communicating with applicants, we support the idea of substituting email communications for paper where possible.

d. Credential Application.

Notification of Receipt: During the pilot program, there were times when the applicant was not notified that the enrollment center had received the card from the production facility. We suggest TSA include email notifications to the applicant when the card is shipped to and received at the enrollment center.

Alternate Processes: In theory, we support the idea that an applicant could designate a specific enrollment center for credential pick up. We would recommend that this be tested prior to formal program rollout. However, we would not support such capability if it would delay program implementation or increase the cost of the card to the applicant. As an alternative, since the card is locked prior to shipment from the production center, the applicant could designate that

the card be mailed to his/her home or place of employment, after which he could take the card to any enrollment center for activation.

e. Using TWIC

Validating the biometric: We suggest TSA include a mechanism for a vessel/facility operator to capture the biometric from the card or from the TSA database for storage in the local database. If this option were available, the vessel/facility operator would be able to validate an individual's identity by matching his fingerprint with the biometric stored in the local database in the event the individual leaves his card home on a given day.

Notification of Invalidation: If a vessel/facility opts to notify TSA when it grants access privileges, TSA should notify the operator if a card belonging to an individual who had been granted access is invalidated. Although we understand this is the TSA's intention, it was not included in the description. This information does need to be included and appropriate electronic information documentation provided.

b. TWIC in Other Modes of Transport. We support the concept that individuals who need access to secure areas of multiple modes of transport only be required to obtain and pay for one interoperable card. While it may not be practical to mandate the use of TWIC in other modes in the near future, it should be relatively simple to allow for use of a TWIC for access at rail, truck or air facilities/conveyances. Similarly, if a truck driver has already undergone screening for an airport security card, this should be accepted at maritime facilities as well. Ultimately, DHS should transition all security programs into a single common credential.

IV. Advisory Committee Participation

It is clear from the Proposed Rule that the NMSAC recommendations were thoroughly evaluated; we appreciate the opportunity to have participated in the process and the consideration given to the recommendations.

G. Enrollment: The answer included in the NPRM did not respond to the NMSAC recommendation that trusted agents undergo financial and credit screening. Does TSA intend to implement this screening? If no, why not?

N. On-Site TWIC Implementation: We agree that after initial challenges were overcome during the prototype that the TWIC did indeed accelerate access to certain facilities. However, since the program was obviously tested on a small scale, and did not include any interaction with the TSA database, it cannot be assumed the same results will accrue directly after full program deployment. We remain concerned that delays at vessel gates will occur due to technical difficulties and suggest that further testing be completed with the initial rollout before committing to subsequent deployment locations and dates.

It cannot be stated strongly enough that minimizing delays at facility gates is paramount. As an additional suggestion, we believe TSA should provide a mechanism for an applicant to request access control at one or more facilities through the web portal. TSA could then forward the requests to the appropriate facilities. Like the pre-enrollment function, this feature would minimize the amount of time spent validating TWIC information the first time an individual arrives at a facility to request access.

Part 1515 – Appeals and waiver processes.

Part 1515.5(c)(6)(d)(1)(iii)/(2)(iii). We strongly question the requirement that the FMSC will be notified if TSA serves a Final Determination of Threat Assessment on an applicant. This raises serious privacy concerns and provides no additional security enhancements. How, for example, will the FMSC use this information? If an individual is denied a TWIC, then he or she simply will not be granted unescorted access by any vessel/facility officer. This will negate the need for FMSC involvement. If FMSC involvement is deemed necessary, then the FMSC should only be notified if an individual has failed to obtain a TWIC as a result of conviction of one of the permanent disqualifying offenses only and is truly considered an immediate terrorist threat.

Part 1572 – Information required for a TWIC Security Threat Assessment.

Part 1572.17(e). If the changes to 33 CFR Part 103.305 (AMSCs) are finalized as proposed, the statement included in section (e) of this Part should be rewritten to include “; or a member of an Area Maritime Security Committee.” However, we have commented to the Coast Guard docket that AMSC members should not be required to obtain TWICs.

Part 1572.19 – Applicant responsibilities for a TWIC Security Threat Assessment.

Part 1527.19(f) – Lost or Stolen Credentials. During the TWIC prototype program, an individual was required to appear at an enrollment center to report a lost or stolen card. This may not be possible or practical in any timely manner after final TWIC implementation, dependent on the number and locations of enrollment centers. We suggest that an individual be able to request that a new card be processed through a secure web portal, submit electronic payment information, and request a new card be produced at that time. The individual would then be required to validate his or her biometrics against the new card at the enrollment location, requiring only one trip to the enrollment site, and saving time for both the applicant and the government.

In the preamble, TSA notes that during the prototype phase, the card production facility printed and shipped replacement cards within 24 hours. An informal survey of Delaware River pilot participants indicated that the timeframe was closer to two weeks before the individual was notified that the replacement card was ready for activation. It is important that a mechanism be available for the individual to continue to access the facilities where he/she has been granted

such access during the period between notification of lost, stolen or damaged card and receipt of replacement.

Part 157.21(d)(3) – Procedures for TWIC Security Threat Assessment. We do not believe the employer, and certainly not the FMSC, should be notified that an individual has received an Initial Determination of Threat Assessment and Immediate Revocation. More often than not, it is likely an individual's failure to meet the assessment standards will be caused by administrative error rather than true security risk. Publicizing such failure would unduly stigmatize the applicant, who at such time would not have had the opportunity to correct his/her records. The employer should only be notified if an individual does not respond to such notice and/or at the time a Final Determination of Threat is issued.

Part 1572.41 – Compliance, Inspection and Enforcement. While we recognize the need for TSA to oversee trusted agents, we do not support a separate TSA vessel/facility inspection program. TSA does not need to inspect the performance of the credential in a variety of circumstances; normal operations will provide more than sufficient assessment opportunities. Similarly, we believe the TWIC system should be designed to provide statistical information with regard to trusted agent performance, and there is no doubt applicants will inform TSA in those instances where the enrollment or activation processes do not perform appropriately. Adding yet another vessel/facility inspection program will only increase costs for both the operators and the government. Rather, the Coast Guard should add TWIC compliance to its existing vessel/facility inspection program.

SUBPART B – Qualification Standards for Security Threat Assessments.

Part 1572.103(a) – Permanent Disqualifying Offenses. We agree that an individual convicted of those crimes listed in section (a)(1-4) should be permanently disqualified from receiving a TWIC. We further agree that the offenses listed in (a)(5-10) are indeed very serious; however we do not believe they should be permanently disqualifying. For example, an individual may be convicted of improperly transporting a hazardous material simply for improper placarding; this does not make him a security risk. Similarly, as egregious a crime as murder may be, it does not indicate the individual is a transportation security threat. Individuals convicted of these offenses should be provided with an opportunity to request waivers.

Part 1572.103(b) – Interim Disqualifying Offenses. As with (a)(5-10), we believe it may not be appropriate for an individual convicted of the crimes listed in this section to obtain employment in the maritime industry; however this decision should be left to the potential employer. We do not believe that these crimes in and of themselves should prevent an applicant from obtaining a TWIC as they do not necessarily point to any national security risk.

Part 1572.105 – Immigration Status. Given that many Canadian and Mexican drivers must enter secure U.S. maritime areas, we support the concept that these drivers be eligible to receive TWICs. We suggest this be extended to railroad employees as well. It is possible that U.S.

citizens will also need to comply with similar Canadian/Mexican programs as they are established. Accordingly, it is important that TSA work with its counterpart agencies in those countries in an effort to create interoperable credentials/systems.

Part 1572.107(b) – Other Analyses. TSA should not have the ability to consider convictions not specifically stipulated as disqualifying or any period of incarceration longer than 365 days in making a determination of an individual's security risk status. These types of analyses are far too subjective across TSA personnel, and even individual TSA employees may derive different assessment results on different days.

SUBPART F – Fees for Security Threat Assessments for TWIC

Part 1572.503(a)(1)(i). We appreciate the challenges to TSA and Coast Guard in attempting to estimate the number of potential TWIC applicants, appeals and waivers. We also appreciate the efforts TSA and Coast Guard have made to combine functionality across programs in an effort to reduce the number of required screenings and therefore the costs of implementing additional security measures.

However, the \$45-\$65 Information Collection/Credential Issuance and the \$50-62 Threat Assessment/Credential Production fees are simply too high and far too large a percentage of the total TWIC costs. We are aware of private vendors who offer similar screening and programs for far less per card; this without the significant volume discounts we assume TSA would be able to obtain under a program of this magnitude. The card production and issuance fees should be separated from the information collection and threat assessment expenses. The applicant should only be required to pay for those card specific services he uses: information collection and threat assessment. Applicants should not be required to fund the TSA infrastructure costs of card production and issuance and program management; this should remain the responsibility of the federal government.

Further, all TWIC applicants should not be required to assume the TSA's costs for adjudicating security threat assessments or administering the appeal and waiver processes. Rather, if the regulated public is required to fund these costs, rather than the federal government, then only those individuals who undergo those processes should be required to pay for them.

Over the last several years, the regulated public has been compelled to implement a wide array of security improvements, including fencing, lighting, personnel training, access control systems, increased electronic data reporting, and other supply chain and transportation security measures. Further, it is likely that most employers, rather than the applicants, will pay for the TWIC costs for the employees, and in the case of non-profit associations such as seafarers' organizations, their volunteers. For example, one local seafarers' organization estimates an \$8,000 first year cost to provide TWICs for its volunteers; this represents an overwhelming 8% increase in the organization's operating budget.

Given the significant increase in the costs of doing business in general, (e.g. insurance, energy) in addition to the added financial burdens associated with costs of enhanced security, we believe DHS should make every possible effort to keep the costs of the TWIC as low as possible for the regulated public.

VII. Rulemaking Analyses and Notices

Impact on Small Business: We believe the fact that TSA and Coast Guard have yet to determine the impact on small business is significant (ref. of seafarer's organization above). If such impact were known, it is likely that some of the processes and requirements outlined in the proposed regulation would demand modification. Other examples are included elsewhere in this document (e.g., tug operators).

We believe the initial costs are significantly understated. For example, the card reader installation costs are estimated at \$200 (at all ranges). In the Philadelphia area, technicians generally charge between \$150 and \$200 per hour, depending on the level of complexity. This estimate would not come anywhere near actual installation, configuration and testing expenses for the card readers. In addition, since readers will be required on both inbound and outbound lanes at facilities, as well as at some areas within the vessels/facilities, or portable readers to be used at waterside access sites, we believe the card reader purchase expense estimate is far too low. The increase in costs associated with the recordkeeping requirement of \$2,709 will not cover the purchase of additional primary and backup storage devices, necessary database development, or operations personnel expenses. In addition, the estimate does not include: programming costs, which can be significant, to integrate the readers with internal access control systems; ongoing equipment maintenance costs; and increased telecommunications expenses resulting from the interaction with the TSA database.

The proposed regulation assumes that some port facilities will be in the position to provide space and utilities for TWIC enrollment centers for an unspecified period of time, some potentially permanently. The direct costs and opportunity costs for these facilities are not included in the estimate.

Other costs: DHS must consider the integration of TWIC with other requirements, such as port authorities who also operate mass transit systems or airports. These agencies may potentially be required to replace large legacy systems to incorporate the TWIC in order to maintain internal consistency and eliminate the expensive redundancy associated with credentialing their own workers.

GENERAL COMMENTS

In general, the items included in the proposed rulemaking were anticipated, and there were very few surprises. However, we believe the devil will be in the details and would like additional information about the specifics of the program deployment, systems testing and implementation.

In addition to the issues and suggestions cited elsewhere in this document, the Maritime Exchange also offers the following concerns.

Timing: For the last four years, industry has consistently questioned the ongoing delays associated with implementing this program. Now it appears that TSA and Coast Guard are now rushing to meet various mandates. We are concerned that this approach will result in the deployment of a critical program which has not been subject to appropriate forethought or testing, as described herein. As a result, we suggest that TSA limit the first group of ports slated for initial rollout to a very small number, similar to that used during the pilot program. The ports selected should include a diverse array of types of facilities (e.g., containers, bulk, breakbulk, ro-ro). However, unlike the pilot program experience, there should be 100% participation in the regions selected. This will provide the opportunity to fully test the new technologies and processes to be implemented under TWIC at a manageable level and in a controlled environment before beginning national deployment. Although this smaller initial rollout is indeed the formal, mandatory implementation of the TWIC program, because such a significant number of untested processes remain, we believe the activities associated with initial rollout should be deemed as testing/research and accordingly funded through DHS R&D programs.

Technologies/Processes: During the course of the TWIC pilot program, TSA intended to test both various technologies as well as the host of business processes that must be developed in order to implement the program. Many of the business processes were not tested, including, but not limited to:

- **Communication with the central database.** It is a significant concern that this functionality was never tested. Having developed a number of data exchange systems over the last 20 years, the Maritime Exchange has a long history and thorough understanding of what can be required to successfully implement these types of projects. From database design and development, user interface design and screen functionality programming, communications scripting, data encryption, and a host of other processes, we are concerned that the lack of testing in a pilot environment will hinder the successful deployment of the program and result in significant delays at facility gates.
- **Hotlisting.** Since no connection between a central database and the individual facilities was established, the card hotlisting process could not be tested.
- **Use of Biometrics.** The prototype did not test use of biometrics with workers at port facilities. This is a significant concern as there is no evidence that the fingerprint will suffice as a biometric in a maritime environment.
- **Interoperability.** One of the original components of the TWIC vision included its ability to be used with legacy systems and across modes. This test was not completed.
- **Web portal.** While the pre-enrollment web was established and used throughout the pilot program, a great deal of the critical functionality was never included. In addition to the concern outlined above regarding individual vs. sponsor access to the portal, pilot program participants were never provided with the capability to request card deactivation through the portal.

- **Background checks.** While pilot program participants did undergo certain screening, full criminal history background checks were not included. As a result, there is no empirical data to determine what the affect of this program may be on the maritime workforce. We believe moving ahead without this knowledge may result in the imposition of a significant barrier to international trade, despite the statement to the contrary in the rulemaking.
- **TWIC issuance to mariners.** Mariners may be away from their home regions for extended periods of time and often require access to various vessels and ports, ferry terminals and other secure facilities. This is a fairly significant portion of the population that was not included in the test.
- **Tests on vessels.** That the TWIC was not tested on vessels, which will rely on wireless telecommunications access, is a significant concern.

Data Integrity: There have been any number of instances over the last several years, such as those involving banks, security screening organizations, and most recently the Veterans Administration, where the security of sensitive personal information, such as that which will be collected and stored under the TWIC program, has been compromised. We are aware that on at least one occasion during the TWIC pilot program, the confidential status of some applicants' data was in question. We ask that DHS provide additional information on the steps it will take to protect the information collected and maintained through the TWIC program.

Communications: During the interim between the August 2002 East Coast pilot program launch and the May 2006 publication of the proposed rule, TSA has not done an acceptable job of keeping the maritime industry informed about program progress. A similar deficiency moving forward to implementation will jeopardize TSA's success in program deployment as well as the ability of the regulated public to comply. The types of communications necessary range from installation and operation schedules at individual sites, to changes in trusted agent personnel, to decisions made regarding technologies and operations.

We suggest DHS continue to work with the pilot participant partners and the NMSAC Credentialing Work Group as a vehicle to provide program updates, seek input, and make decisions. In addition, DHS should invite all commenters to this docket to be members of an email distribution group (and/or Homeport website community) and provide updates, preferably weekly but not less than monthly.

TWIC Leadership: Because of the high level of employee turnover with DHS, the TSA, the TWIC program office and the contractors during the course of the pilot program, we are concerned that DHS may not be in a position to put together a team of talented individuals who will see this project through to completion. Failure to do so will undoubtedly result in further program delays and cost increases, and we seek some assurance from DHS that it has a plan to prevent the inordinately high turnover historically associated with this program.

Port Worker Screening: With the publication of the TWIC proposed rulemaking, we believe DHS should immediately discontinue the screening program for port employees, longshore

Maritime Exchange for the Delaware
River and Bay
Docket TSA-2006-24191
June 16, 2006
Page 12 of 12

workers and contractors implemented on April 28. This is program that is completely redundant to TWIC and its continuation will unnecessarily consume sorely-needed resources for both the government and the regulated public.

TWIC Potential: TWIC can serve as a building block for a host of commercial and maritime security measures. From a security perspective, TWIC can be added to other systems to further strengthen supply chain security. For example, our Maritime On-Line system, which is a community-wide maritime information and intelligence system, currently provides vessel and facility operators with Customs & Border Protection cargo status messages. Through this system, vessel operators, importers, and/or their agents, can provide cargo release information to facilities and assign trucking companies to certain shipments, which is then relayed to facility operators. By incorporating TWIC into this process, when a driver arrives at a marine facility gate, the TWIC can help prove that the driver is authorized to haul the cargo listed on his delivery order documentation. From a commercial perspective, the TWIC can be used to store training information, certifications, and drug and alcohol testing results, vessel assignment information, thus eliminating the need for separate employee ID cards and the costs associated therewith.

We suggest TSA continue to work with its federal counterparts and industry to explore and take advantage of these opportunities.

Finally, because the implementation of TWIC represents such a sea change in the way maritime commerce is conducted, we believe the Coast Guard and TSA should extend the comment period by an additional 45 days and host further public meetings. The program and its inherent requirements are complex, and even those of us who participated in the pilot program are having difficulty assessing its full ramifications. There are large numbers of international transportation organizations who do not have an understanding of what the program entails or how it may affect their operations; these organizations should be provided with additional information and additional time to complete their assessments.

The Maritime Exchange for the Delaware River and Bay appreciates the opportunity to provide comments to this docket. We look forward to working with both TSA and the Coast Guard to meeting the challenges addressed in this letter and helping achieve the dual goals of meeting security needs and fostering a healthy commercial environment.

Sincerely,



Dennis Rochford
President