



March 28, 2007

**Comments on Transportation Worker Identification Credential (TWIC)
Biometric Reader Specification and TWIC Contactless Smart Card Application**

Docket: USCG-2007-27415

The Maritime Exchange for the Delaware River and Bay is a non-profit association representing port and maritime interests in Southeastern Pennsylvania, Southern New Jersey and Delaware. On behalf of our nearly 300, members, the Maritime Exchange is writing to express its strong support for the National Maritime Security Advisory Committee (NMSAC) "Recommendations on Developing a Contactless Biometric for the TWIC." Specifically, the Exchange believes the Department of Homeland Security should adopt the technical specification listed as Appendix III as well as the other recommendations approved by the NMSAC. We do not support the "Alternate Option" described in Appendix IV.

The Maritime Exchange has long been an advocate for TWIC and continues to stand behind the program. Our rationale for supporting the NMSAC position is that it remains consistent with the original TWIC vision: If implemented correctly, the TWIC can be a tool to improve transportation security while not unduly jeopardizing international commerce and while protecting individual privacy. The contactless reader specification recommended by NMSAC will meet each of these important goals.

On the other hand, increasing the complexity of the TWIC program by encrypting the fingerprint template (as outlined in the "Alternate Option") will not measurably improve privacy protection, nor will it enhance security at maritime facilities. It will, however, be detrimental to port operations and thus to U.S. commerce. The bottom line, as stated in the NMSAC recommendations, is that "an individual interested in 'stealing' a fingerprint would meet much less technical resistance and obtain a more accurate representation by lifting it from an object in a public place such as a car door, window or drinking glass," than he would from a template obtained from a TWIC contactless biometric transfer.

In essence, the technology to reengineer a fingerprint from a template is not available. Though we understand the desire to attempt to circumvent technologies which may be developed in the future, the severe operational impacts which will accrue as a result of any decision to require that the fingerprint template be encrypted make the decision an extremely imprudent one for DHS. These impacts include issues associated with managing keys, increased processing time at facility gates, and increased potential for TWIC verification failure – all of which would increase costs of international commerce and divert security resources unnecessarily.

Should such technology be attained in the future, it is extremely likely that DHS could add additional security features to TWICs, just as the Department is now considering adding functionality to TWIC cards issued under the current rulemaking to accommodate the contactless read of the TWIC once it is developed. In short, the United States simply does not have the luxury of implementing costly measures to protect against a threat which does not exist in today's environment.

Additional information is provided below in response to the questions posed in the Notice.

1. Should additional security measures be included in the specifications, such as the use of a PIN, to further minimize the chance that a fingerprint template from a lost or stolen credential could be obtained by an unauthorized individual? If so, would the addition of a PIN or other security measure adversely impact operations? Does the length of the PIN affect adverse impacts in any measurable way?

We agree with the NMSAC that a PIN should not be used in the TWIC authentication process. The sheer numbers of people who move through facility gates, a large percentage of whom enter facilities at approximately the same time, makes this feature impractical. The likelihood is that individuals will a) either forget their PIN numbers and/or b) write them down where they can be lost or stolen. Both of these scenarios detract from the potential security value a PIN affords. In addition, given that TWICs are to be presented by drivers (and passengers) entering facilities in their vehicles, there does not seem to be any reasonable way for the individual to swipe a card, present a fingerprint, and enter a PIN. This is particularly relevant given that 85-92% of the population is right handed and readers at vehicle gates will of necessity be on the driver's left hand side. The length of the PIN is not particularly relevant as it relates to these concerns, however a longer PIN would undoubtedly increase the incidence of input errors and increase processing time.

2. What, if any, privacy concerns exist if the fingerprint template is obtained by an unauthorized individual?

See above discussion. Because the fingerprint template is not a fingerprint image, there is little concern that it could be used fraudulently if it were stolen. Simply put, encrypting a fingerprint template is a jackhammer solution to a thumb tack problem.

3. How would the recommended specifications impact facility and vessel security and operations?

It is our expectation that requiring individuals to undergo security assessments will improve transportation security. However, implementation of the TWIC program in any configuration will have a dramatic impact on maritime operations. We believe the specification recommended by NMSAC will minimize the detrimental impact the program will have on port and vessel operations.

4. How would the recommended specifications impact existing physical access control systems?

To the extent that certain facilities have implemented automated access control systems, the readers identified in both appendices will require an interface with both the TSA and between the reader(s) and the individual facility systems. The Maritime Exchange continues to believe that TSA should accommodate legacy systems where possible, and if the TWIC program is such that existing systems must be replaced, the TWIC rollout should provide an opportunity for facilities to phase-in use of equipment as legacy systems reach the end of their useful lives.

5. Are there alternative designs we should consider, and if so, what are the advantages and disadvantages of the alternative designs?

As indicated in the NMSAC recommendations, there may be other approaches to encrypting the fingerprint template than those contained in either Appendix III or VI. Given that NMSAC has

concluded “that the operational complexities increase by a level of magnitude and to the point where they are not proportionate with any perceived benefit of encrypting the biometric template. In short, there is no empirical evidence that encrypting the fingerprint template affords any additional protection of personal privacy,” the Maritime Exchange does not believe DHS should waste its resources considering alternatives.

6. How would the recommended specifications impact product, system, and operational costs?

As stated previously, the NMSAC recommendation will minimize costs of implementing and using the readers compared to the alternative. Additional costs will be dictated by policy decisions yet to be made by DHS (such as method and frequency of “hot list” updates, use of readers at low-risk vessels and facilities, data storage requirements, etc.)

7. How quickly could the recommended specifications be incorporated into the design and manufacture of access control equipment?

The Maritime Exchange is not in a position to answer this question.

8. Should there be a process for identifying a Qualified Products List (QPL) or other equivalent regime? If so, what is the most efficient and effective way of creating a QPL?

We agree that DHS should develop a QPL, which will provide assurance to the regulated public that the products they are purchasing have been tested and meet program guidelines. DHS should work with the security/technology industry to develop such a process.

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,

A handwritten signature in black ink that reads "Dennis Rochford". The signature is written in a cursive style with a long, sweeping horizontal stroke at the end.

Dennis Rochford
President