

General Observations and Comments on TWIC Reader NPRM

Readers Required Only for Risk Group A

The major news in this NPRM is that only those facilities and vessels in Risk Group A are required to have TWIC readers at all access points. These operators handle Certain Dangerous Cargo (CDC) or otherwise meet the highest risk for inclusion into this category. This encompasses only 532 facilities and 38 vessels vs. the anticipated requirement for use of TWIC readers by operators in Risk Groups A & B - which would have encompassed 2,178 facilities and 38 vessels.

It was noted that this initial requirement for readers only in Risk Group A is described as a “phased” approach and the Coast Guard reserves the right to issue proposed rules for public comment in the future that will require readers for Risk Group B.

One of the consequences of this “phased” approach will be to substantially reduce the potential market for TWIC readers which may make it impractical for reader manufacturers to incur the cost of QTL testing and designing their reader hardware and software products to specifically conform to the TWIC Reader Hardware and Card Application specification.

It was also noted that container terminals are generally included in Risk Group B. These facilities were considered to be one of the most likely users of TWIC readers. While it is disappointing that such facilities may not be required to have TWIC readers, it is possible that they may wish to implement them anyway for economic reasons. While the NPRM does not acknowledge or refer to the economic savings associated with TWIC readers, such savings can be substantial when you consider the personnel cost of performing visual inspection of TWIC cards at each entry point. Container terminals generally have the highest number of entry points because of multiple truck lanes and pedestrian gates.

It is believed that the Coast Guard ignored the economic benefits of TWIC readers at such facilities and did not consider the offset of security personnel labor for visual inspection vs. the amortized capital cost of implementing TWIC readers. This is an area for potential comment.

It was noted that the NPRM included a provision stating that owners and operators would have the discretion to impose access control measures that are stricter than the minimum regulatory requirements. The NPRM specifically states that “for now, vessels and facilities that do not present this heightened risk would either continue to visually inspect TWICs or voluntarily deploy TWIC readers”.

It was noted that the NPRM is seeking public comment on any additional costs or benefits to TWIC reader requirements not accounted for in the NPRM. It may be appropriate to comment on the potential labor savings for security personnel that would otherwise be required to perform visual inspection if readers were implemented in Risk Group B facilities.

Compliance Deadline

Owner operators are required to amend security plans to include TWIC reader requirements within two years following publication of the final rule. Assuming that the final rule is published within a year, the reader requirement would not go into effect until early 2016 – nine years after the first TWIC cards were issued.

Required Readers Must Always Perform Biometric Verification

There is no provision for limited functionality modes of TWIC readers for Risk Group A. Readers must perform all three modes including: Biometric check for identity verification, card authentication and card validation for each access event.

No Requirement for Reader Mode Changes at Elevated MARSEC Levels

It was noted that the NPRM states that the Coast Guard does not believe that elevated TWIC reader requirements at higher MARSEC Levels are generally practical or appropriate. The only impact to higher MARSEC requirements is the necessity to refresh the Cancelled Card List (CCL) daily at higher MARSEC threat levels rather than weekly.

Exception Handling

If a TWIC holder has unreadable fingerprints, there is a provision for using PIN or alternate biometric. It can be assumed that the PIN can be a PACS PIN managed by the owner operator through their PACS rather than the TWIC card PIN. The NPRM expects owners and operators to describe the exception handling process to be used in such cases in their security plans.

No Requirement for PINs

The NPRM does not propose a requirement that TWIC-holders enter their PINs in order to access secure areas. However the NPRM states that mariners must provide TWIC PIN information to Coast Guard personnel upon request.

Further, the NPRM states that “owners and operators may choose to impose their own PIN verification requirement on individuals before granting them access to secure areas”.

Support for Alternate Biometrics

The NPRM states that an owner operator may “(1) use a TWIC reader to match the TWIC-holder’s fingerprint to one of the fingerprint templates stored in the TWIC; or (2) use a PACS to match the TWIC-holder’s biometric to the biometric stored in a PACS. For the latter option, owners and operators may use a different biometric than the fingerprint, such as an iris scan or hand geometry, stored in a PACS to be matched to the individual seeking access to secure areas.”

The term “Biometric Match” is defined in the NPRM as follows: “a confirmation that: one of the two biometric (fingerprint) templates stored in the TWIC matches the scanned fingerprint of

the person presenting the TWIC; or the alternate biometric stored in a PACS matches the corresponding biometric of the person.”

When using alternative biometrics, the NPRM suggests a requirement to perform PACS registration and link TWIC fingerprint verification to the use of alternative biometrics to create a “chain of trust”. The NPRM states as follows: “If using a PACS, biometrics other than fingerprints may be used to perform the identity verification, provided that the owner or operator links the person, the TWIC, and the alternate biometric in the PACS. To do this, the owner or operator would be required to perform a one-time biometric match and card authentication using a TWIC reader.”

TWIC Readers Must be on the QTL

The NPRM includes a definition of TWIC reader as follows: “TWIC reader means an electronic device listed on TSA’s Qualified Technology List (QTL) and used to verify and validate: the authenticity of a TWIC; the identity of the TWIC-holder as the legitimate bearer of the credential; that the TWIC is not expired; and that the TWIC is not on the CCL.”

Record Keeping

Owners and operators using TWIC readers, with or without a PACS, would be required to maintain certain records of access transactions for at least 2 years.

Public Meetings

The Coast Guard will hold at least one public meeting regarding the NPRM and possibly more. The date and location for such meetings will be published in the Federal Register in a separate notice.