TWIC/MTSA POLICY ADVISORY COUNCIL

MARCH 15, 2011

Policy
Voluntary Use of TWIC Readers

01-11

Issue – In accordance with the Maritime Transportation Security Act (MTSA) and Security and Accountability for Every (SAFE) Port Act, it is clear that Congress intended the use of transportation security card readers to leverage the full security benefits of Transportation Worker Identification Credential (TWIC). The Department of Homeland Security (DHS), the U.S. Coast Guard, and the Transportation Security Administration (TSA) are still developing TWIC reader requirements as the reader pilot progresses. As such, many facility owner/operators who received grant funding have been reluctant to move forward on purchasing TWIC equipment.

Background – A TWIC Notice of Proposed Rulemaking (NPRM), which included both credential and credential reader requirements, was published on May 22, 2006. Based on public and stakeholder input, DHS decided to split the final rulemaking and removed the reader requirements to be considered in a future rulemaking once contactless reader capabilities for TWIC could be established. That future rulemaking will cover a much broader range of issues related to TWIC readers than does this policy, including but not limited to specific card authentication, validation and identity verification requirements. The TWIC Final Rule implementing the credential requirements published on January 25, 2007.

On July 2, 2007, the Coast Guard published Navigation and Vessel Inspection Circular (NVIC) 03-07, GUIDANCE FOR THE IMPLEMENTATION OF THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROGRAM IN THE MARITIME SECTOR. The purpose of this guidance document was to prepare and assist field units and industry partners for compliance with the TWIC Final Rule. It included a discussion on how to incorporate the TWIC requirements from the Final Rule into existing physical access control systems (NVIC 03-07, enclosure 3, page 15).

After encountering requests for clarification on this guidance, the Coast Guard published Policy Advisory Council (PAC) Decision 08-09, Incorporating TWIC into Existing Physical Access Control Systems - Change 1 on August 31, 2009. PAC Decision 08-09 Change 1 provided guidance explaining that the Coast Guard viewed as TWIC compliant vessels or facilities with existing electronic physical access control systems that continue to use company-issued local access cards for entry, as long as the system supports a match between the local access card and the individual's valid TWIC upon each entry. At that time, use of existing electronic card readers, designed to work with the TWIC, was authorized to meet the requirements for card authentication and card validity (33 CFR 104.265(c)(1)(ii) & (iii), 105.255(c)(1)(ii) & (iii), or 106.260(c)(1)(ii) & (iii)).

Identity verification, in which a match of the photo on the TWIC is compared with the individual presenting the TWIC, had to be performed separately (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i) or 106.260(c)(1)(i)). Matching the biometric template stored on the TWIC to the TWIC holder's fingerprint as the sole process to verify identity was not authorized at that time.

The SAFE Port Act requires DHS to conduct a card reader pilot program to test the business processes and technology required to deploy transportation security card readers as well as examine operational impacts for vessel and facility owners and operators. It also requires a report to Congress that provides the results of the pilot. The statute further requires any final TWIC reader rule be consistent with the findings of the pilot program. DHS will issue an NPRM incorporating the data and conclusions into the proposal and its supporting analyses. This will satisfy the SAFE Port Act requirement, and ensure the public has time to comment on the proposed rule before DHS publishes a final rule. (Initial government testing and evaluation of available TWIC readers has been completed; but additional testing of new readers is an ongoing process. Additionally, there are owners/operators who have been awarded DHS Port Security Grants for the purpose of purchasing and installing TWIC readers and systems, whose funding will expire if it is not expended before 2012).

For these reasons, the Coast Guard has re-examined the capability for TWIC readers to verify identity, using biometric match, in a manner that may be deemed equivalent to the visual card inspection requirements in 33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i), and 106.260(c)(i).

Policy – All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with 33 CFR §101.514. At each entry, the TWIC must be checked for: (1) identity verification, (2) card validity, and (3) card authentication.

(1) Identity verification ensures that the individual presenting the TWIC is the same person to whom the TWIC was issued. The current requirement for identify verification is to compare the photo on the TWIC to the person at the access point (33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i)), or 106.260(c)(1)(i)).

In accordance with 33 CFR §101.130, the Coast Guard determines that a biometric match using a TWIC reader from the TSA list of readers that have passed the Initial Capability Evaluation (ICE) Test (available at: http://www.tsa.gov/assets/pdf/twic_ice_list.pdf) to confirm that the biometric template stored on the TWIC matches the fingerprint of the individual presenting the TWIC meets or exceeds the effectiveness of the identity verification check.[1]

(2) Card validity involves the determination that a TWIC has not expired; been reported lost, stolen, or damaged; or been revoked for cause by TSA. The current requirement for

[1] Any TWIC reader authorized by this guidance to meet the identity verification requirement at 33 CFR 104.265(c)(1)(i), 105.255(c)(1)(i)), or 106.260(c)(1)(i) may no longer be valid after the promulgation of a TWIC reader final rule requiring the use of readers during access control procedures.

card validity is visual inspection to check that the TWIC has not expired (33 CFR 104.265(c)(1)(ii), 105.255(c)(1)(ii), or 106.260(c)(1)(ii)).

In accordance with 33 CFR §101.130, the Coast Guard determines that using a TWIC reader to check for card validity by either[2]:

(a) comparing the card's internal Federal Agency Smart Card Number (FASC–N) to the TSA Cancelled Card List or
(b) using a Certificate Revocation List (CRL) meets or exceeds the effectiveness of the card validity check.

(3) Card authentication ensures that the card being used is an authentic TWIC. The current requirement for card authentication is visual and/or physical inspection of various security features present on the card (33 CFR 104.265(c)(1)(iii), 105.255(c)(1)(iii), or 106.260(c)(1)(iii)).

In accordance with 33 CFR §101.130, the Coast Guard determines that card authentication with a TWIC reader to perform the CHALLENGE/RESPONSE protocol using the Card Authentication Certificate and the card authentication private key on the TWIC meets or exceeds the effectiveness of the card authentication.[3]

(4) Owners/operators using biometric readers that are on the TSA list of readers that have passed the Initial Capability Evaluation (ICE) Test should ensure that the readers are operated and maintained according to manufacturer's instructions; and operated by individuals who are trained in the use of said readers.

(5) Any vessel or facility owner/operator using the above provisions must submit a Vessel Security Plan or Facility Security Plan amendment to the Marine Safety Center, cognizant Captain of the Port, or District Commander in accordance with 33 CFR 104.415(a), 105.415(a), or 106.415(a). The amendment must detail the implementation of a TWIC reader system as an equivalent access control procedure to the one established by 33 CFR 104.265(c)(1), 105.255(c)(1), or 106.260(c)(1), as applicable.

(6) PAC Decision 08-09, Incorporating TWIC into Existing Physical Access Control Systems - Change 1, remains valid for vessels or facilities with existing electronic physical access control systems as long as the systems can support a match between the local access card and the individual's valid TWIC upon each entry. PAC Decision 08-09 allows owners and operators to use existing (non-TWIC) electronic cards, readers, and physical access control systems to meet the requirements for card authentication and validity ONLY. Visual inspections of the TWICs at the prescribed rate would still be required.

[2] Any TWIC reader authorized by this guidance to meet the card validity requirement at 33 CFR 104.265(c)(1)(ii), 105.255(c)(1)(ii), or 106.260(c)(1)(ii) may no longer be valid after promulgation of a TWIC reader final rule on access control procedures.

[3] Any TWIC reader authorized by this guidance to meet the card authentication requirement at 33 CFR 104.265(c)(1)(iii), 105.255(c)(1)(iii), or 106.260(c)(1)(iii) may no longer be valid after promulgation of a TWIC reader final rule on access control procedures.

Note: TWIC readers allowed pursuant to this interim guidance may no longer be valid after promulgation of a TWIC reader final rule requiring the use of readers during access control procedures. DHS will not fund replacement readers. Any grandfathering or phase-in period considerations will be addressed in the rulemaking process, providing adequate opportunity for comment, but should in no way be inferred from this interim guidance.