TWIC/MTSA POLICY ADVISORY COUNCIL

July 15, 2009
Updated August 31, 2009

Policy
Incorporating TWIC into Existing Physical Access Control Systems

08-09 Change 1

Background – 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 which was published on January 25, 2007.

Incorporation of the TWIC into Existing Physical Access Control Systems was addressed in NVIC 03-07, enclosure 3, page 15. However, in response to recent feedback from field units and industry regarding the potential for misinterpretation of this section, this Policy Advisory Council (PAC) decision provides additional clarification and policy pertaining to this issue.

Discussion – Incorporating TWIC into existing physical access control systems – The intent of NVIC 03-07 section 3.3.f (page 15) was to allow vessels or facilities with existing electronic physical access control systems to temporally continue to utilize their company-issued local access cards for entry while final regulations for TWIC card readers were developed. The NVIC authorized use of the existing electronic physical access control system, as long as the system can support a match between the local access card and the individual's valid TWIC upon each entry. The desired benefit to owners/operators was the ability to continue to use a system that was already in place, prior to full TWIC implementation utilizing credential readers, which interfaced with a local access badge.

Title 33 Code of Federal Regulations (CFR), Parts 104.265(c)(1) and 105.255(c)(1) require the owner or operator to implement TWIC into their access control measures and ensure that persons seeking unescorted access to secure areas of their vessel or facility present their TWIC for inspection prior to authorizing entry. The owner/operator's TWIC inspection must include: a match of the photo in the TWIC to the individual; verification that the TWIC has not expired; and a verification of the various security features of the credential. Vessel and facility owner/operators who elect to utilize the provisions of NVIC 03-07 section 3.3f are considered to be meeting only the card authentication and card validity requirements found in 33 CFR, Part 104.265(c)(1)(ii) & (iii) or 105.255(c)(1)(ii) & (iii), as appropriate.

The example provided in 3.3.f states the "TWIC does not need to be used as a visual identity badge for each entry." This is still the USCG policy; however, identity verification of the individual utilizing a company credential or access card is still required before unescorted access may be granted to secure areas, as is stated in section 3.3.a of the NVIC, and in accordance with 33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i), as appropriate. Verification is necessary to ensure the company card is not being utilized by another individual who may be unauthorized. This verification could be accomplished via gate guard, Closed Circuit Television (CCTV) or other means acceptable to the relevant Coast Guard Captain of the Port (COTP).

The aim of the Coast Guard remains the same. The Coast Guard seeks to enhance the security of ports and vessels by ensuring that only persons who hold valid TWICs are granted unescorted access to secure areas of MTSA regulated vessels and facilities.

Policy – Coast Guard policy surrounding sections 3.3.a and 3.3.f of NVIC 03-07 is as follows:

1. Owners/operators must be capable of demonstrating to Coast Guard inspectors that issuance of a unique local access card to an individual, allowing the individual unescorted access into the secure area of the vessel or facility, is tied to verification of a valid TWIC being issued to the individual. Initial verification of the TWIC must meet all of the inspection requirements in 33 CFR 104.265(c)(1) or 105.255(c)(1) (as appropriate). An individual who does not hold a valid TWIC must not hold a company-issued local access card that allows unescorted access into secure areas.
2. Once a TWIC is verified to be valid, and until the Coast Guard publishes a final rule requiring the use of TWIC readers as an access control measure, a company issued local access card can be used for unescorted access to secure areas. Identity verification (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i)), must still be performed to ensure the individual presenting the company issued local access card is the individual authorized unescorted access. This means that a match of the photo on the company card to the individual must occur.
3. Continued use, by an individual, of the company-issued local access card to gain access to secure areas of the vessel or facility is authorized based on the vessel's or facility's verification that the individual's TWIC remains valid in accordance with 3.3.f of NVIC 03-07 prior to authorizing unescorted access to a secure area.
4. Unescorted individuals, who have gained access within a vessel's or facility's secure area using the company-issued local access card, must still be in possession of their TWIC, or be able to retrieve it within a reasonable time, as required by 33 CFR 101.515(d)(1) & (2). If during the check of the TWIC it is found to be invalid, the company-issued local access card to the secure area is also invalid. Appropriate action by the Coast Guard will follow if a person is found to not be in possession of a valid TWIC.
5. Use of existing electronic card readers, designed to work with the TWIC, is authorized to meet the requirements for card authentication and card validity (33 CFR 104.265(c)(1)(ii) & (iii) or 105.255(c)(1)(ii) & (iii)). Identity verification (33 CFR 104.265(c)(1)(i) or 105.255(c)(1)(i)), in which a match of the photo on the TWIC is compared with the individual presenting the TWIC, must still be performed separately. Identity verification can be accomplished by utilizing a

gate guard to match the photo to the individual, use of CCTV to perform the match, or other means acceptable to the COTP. Matching the biometric template stored on the TWIC to the TWIC holder's fingerprint as the sole process to verify identity is not authorized at this time. Government testing and evaluation of currently available readers is on-going and additional regulatory requirements and policy guidance will be needed prior to full utilization of reader capabilities to meet all inspection requirements.

NOTE:

(1) For any **facility that does not meet the provisions of the identity verification in this PAC** due to previously installed access control systems and/or infrastructure (must have been in place prior to July 15, 2009), the following procedures shall be utilized in order to mitigate any potential security risks:
   a. At MARSEC Level 1 –Random checks for TWIC must be conducted of individuals accessing secure areas at the rate specified on the secure (password-protected) side of HOMEPORT at http://homeport.uscg.mil (all inspection requirements under 33 CFR 105.255(c)(1) must be conducted, including the identity verification component).
   b. At MARSEC Level 2 & 3 –Verification at the rate specified on the secure (password-protected) side of HOMEPORT to include identity verification, card validity, and card authentication must be conducted via a company issued badge or TWIC prior to being granted unescorted access to secure areas.
   c. The random TWIC inspection requirements discussed above are in addition to the performance standards for screening found in MARSEC Directives 105-1, 2, & 3.

(2) Any facility utilizing the above provisions must submit an FSP amendment to the cognizant COTP in accordance with 33 CFR 105.415(a) detailing the implementation of these alternate access control procedures.

(3) The above guidance is intended for use during the transition period leading up to the promulgation of a TWIC reader final rule, at which time it is anticipated that use of legacy access control systems that are not compatible with a TWIC will no longer be acceptable for use. Any access control system or infrastructure put in place after July 15, 2009 must be in full compliance with the requirements of 33 CFR 105.255(c)(1).