

TWIC/MTSA POLICY ADVISORY COUNCIL

October 24, 2008

Updated February 20, 2009

Policy

TWIC Activation & Fingerprint Reject Impacts – Limited Equivalent Security Measure

07-08 Change 5

Issue – On October 21, 2008 the government facility that houses the Transportation Worker Identification Credential (TWIC) system experienced a building-wide power outage. Though power was quickly restored, the part of the system that facilitates credential activations was affected. The Transportation Security Administration's (TSA) TWIC Program office has resolved this issue and full activation capability was restored nation-wide by the end of November 2008. The outage and subsequent activation backlog has impacted applicants working in those Captain of the Port (COTP) Zones that have already come into compliance (October 15, 2008, November 28, 2008, December 1, 2008, December 30, 2008, and January 13, 2009, February 12, 2009) and those soon coming into compliance (February 28, 2009) with the TWIC regulations found in 33 CFR part 105, as those without a valid TWIC will be ineligible for unescorted access to a Maritime Transportation Security Act (MTSA) regulated facility.

In addition, some transportation workers who applied for their TWIC between October 2007 and August 2008 were informed by TSA that their fingerprints were rejected by the FBI so their TWIC application could not be completed. Although applicants with fingerprint rejections have been addressed, some individuals have only recently completed a successful security threat assessment and may not receive their credential prior to the start of compliance in their area. Others have been informed during the activation process that a successful one-to-one biometric match could not be obtained and therefore a replacement TWIC needed to be ordered.

Background – 33 CFR 105.255 requires that MTSA regulated facility owners/operators prevent an unescorted individual from entering a secure area unless he/she holds a TWIC. 33 CFR 101.130 allows the Commandant to approve equivalent security measures for any measure required in part 105 as meeting the effectiveness of the required measure.

For an applicant to complete the TWIC enrollment process, applicants must visit the same enrollment center on two separate visits. The first is to enroll for the TWIC and the second is to activate the credential. The Transportation Security Administration (TSA) security threat assessment (STA) is completed before the TWIC is printed; thus the fact that a TWIC has been printed can, temporarily and under significant service disruptions such as the system's inability to provide credential activation services and the associated backlog, serve as proof that an individual has passed the STA even before an individual visits the enrollment center and activates his/her credential.

Discussion – In order to minimize disruptions to maritime operations and commerce within COTP Zones that have begun compliance and those COTP Zones that will soon begin compliance, due to the activation outage, the U.S. Coast Guard and TSA have developed an alternative method for facility owners/operators to use to grant unescorted access to individuals who are currently required to present a TWIC at MTSA regulated facilities.

At the owner/operators discretion, an individual can obtain unescorted access to secure areas of MTSA facilities required to be in compliance with the TWIC provisions of 33 CFR part 105 by providing to facility security personnel:

- 1) a photo ID that meets the requirements of 33 CFR 101.515, and
- 2) proof that their TWIC has been printed and is ready for activation.

Individuals who can prove that their TWIC has been printed and is ready for activation are considered able to show that they have successfully passed the TSA security threat assessment, and therefore do not pose a security threat. Some examples of ways that an individual may prove their TWIC has been printed include, but are not limited to:

- 1) Printing the e-mail, sent by TSA during the notification process, that their TWIC is ready for pick-up;
- 2) Providing the facility security officer (FSO), or other facility employee with security duties, with the individual's TWIC application ID number which then can be used by the facility with the "check card status" feature on www.twicinformation.com (acceptable statuses under this PAC include: Card in Production, Card in Transit, or Card Ready for Activation); or
- 3) Provide the FSO, or other facility employee with security duties, the individual's first name and last name. This information can then be used by the facility to determine the status of the individual's TWIC using the secure (password protected) side of homport.uscg.mil. A list of individuals for each enrollment center who have passed the security threat assessment will be posted under the headings TWIC > General Information > PAC 07-08 List of Individuals. The lists will be updated weekly as individuals complete a successful security threat assessment.

COTPs should work closely with facility owners and operators to ensure that the above policy is implemented to provide equivalent security at MTSA regulated facilities while minimizing impacts on maritime operations and commerce.

Applicability:

This PAC will remain in effect until **February 27, 2009** for the following COTP Zones: Hampton Roads, Morgan City, New Orleans, Upper Mississippi River, Miami, Key West, and St. Petersburg.

This PAC will remain in effect until **March 12, 2009** for the following COTP Zones: Honolulu, Prince William Sound, Southeast Alaska, and Western Alaska.

This PAC will remain in effect until **March 27, 2009** for the following COTP Zones:
Portland, Puget Sound, and San Francisco Bay.

Upon expiration of this PAC for the relevant COTP Zone(s), only individuals with a valid TWIC will be eligible for unescorted access to a Maritime Transportation Security Act (MTSA) regulated facility.