

September 2006

TWIC – a bridge too far

Dennis L. Bryant

On September 17, 1944, thousands of British paratroopers landed up to 100 miles behind German lines in Holland to secure bridges so that Allied forces could circumvent the Siegfried Line and hopefully bring World War II in Europe to a swift conclusion. Unfortunately, Operation Market Garden didn't work out. The bridge at Arnhem proved to be 'a bridge too far' and was outside the reach of supporting ground troops. The Allies were forced to retire and regroup and the end of the conflict was delayed many months, resulting in numerous additional casualties.

The Transportation Worker Identification Credential (TWIC) program may be headed down the same path.

TWIC is mandated by the Maritime Transportation Security Act of 2002 (MTSA). The statute has several very distinct provisions. It broadly defines the TWIC; describes the physical boundaries within which a TWIC is required; designates who is potentially eligible to have a TWIC; identifies persons who may not have a TWIC; and establishes restrictions on use of information obtained during the TWIC application process. The rationale for the TWIC program is somewhat inarticulately stated as follows: This provision "establishes a national standard for issuance of transportation security cards whose purpose is to control access to ensure terminal areas to only authorized personnel."

Like Operation Market Garden, though, the TWIC program has proven to be highly complex and to rely for its success on numerous sub-programs. Many of those sub-programs have failed to deliver as expected and the TWIC program is in serious danger of collapse unless it regroups.

The TWIC program has been in development since 2002, but it was not until May of 2006 that the official Notice of Proposed Rulemaking (NPRM) was published in the Federal Register. That was followed by four hastily-arranged public meetings and a short 45-day comment period. The few public meetings and the short comment period were both heavily criticized by the maritime community.

E-mail

dennis.l.bryant@gmail.com

Internet

<http://brymar-consulting.com/>

Maritime Reporter & Engineering News

<http://marinelink.com/en-US/magazines/Archive.aspx?MID=3>

The MTSA directs that the TWIC include biometric data, but does not define any particular parameters for what data is to be incorporated or how the incorporation is to be effected. TSA has elected to utilize the same Federal Information Processing Standard (FIPS) as has been established for personal identity verification of federal employees and contractors. This decision, when made, was wise, because then the TWIC cards and readers could be based on proven technology.

The biometric data to be collected for the TWIC process would consist of the following: (1) a full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process; (2) an electronic facial image used for printing the facial image on the card as well as for performing visual authentication during card usage; and (3) two electronic fingerprints to be stored on the card for automated authentication during card usage.

The fly-in-the-ointment is that the FIPS program has not been completed. While the basic FIPS standard has been recently approved, numerous details have yet to be resolved before the program can be implemented for its intended audience. It will not be possible to roll out the TWIC program until the underlying structure of FIPS has been fully completed and implemented.

The MTSA directs that the TWIC be used to control unescorted access to the “secure areas” of a vessel or facility that is required to have a maritime transportation security plan. The term “secure area” is not defined in the statute. The NPRM, though, proposes the following definition: “*Secure Area* means the area on board a vessel or at a facility or outer continental shelf facility over which the owner/operator has implemented security measures for access control, as defined by a Coast Guard approved security plan.”

The proposed definition of secure area looks very much like the existing definition of “restricted areas” in the Coast Guard’s maritime security plan regulations. Those regulations include the following: “*Restricted areas* mean the infrastructures or locations identified in an area, vessel, or facility security assessment or by an operator that require limited access and a higher degree of security protection.”

Careful review reveals that the MTSA does not require that the secure area for TWIC purposes be coterminous with the restricted area as established for security plan purposes. It is unclear why the TSA (and the Coast Guard) have elected to not exercise the discretion afforded by the statute and instead to take this broad-brush approach, since it makes the process significantly more complicated and expensive for all involved. For the agencies, this course of action makes highly difficult, if not impossible, compliance with the federal law mandating that regulations be implemented so as to minimize avoidable expenses imposed on small businesses. For US companies that fall into the small business category, it requires expenditure of significant time, personnel, and monies to comply with requirements that will, arguably, provide minimal security enhancements to extremely low-risk facilities and vessels.

As noted by Homeland Security Secretary Michael Chertoff when he announced the port security grants on September 13, 2005, security measures should be considered with regard to a “risk-based formula weighing threat, vulnerability, and consequence. Consequence considers risks to people, the economy, and national security. Vulnerability involves factors such as distance from open water, number of port calls, and presence of tankers. Threat includes credible threats and incidents and vessels of interest information.”

The MTSA directs that, subject to various requirements, the following persons are potentially eligible for a TWIC: (A) an individual allowed unescorted access to a secure area designated in a vessel or facility security plan; (B) an individual issued a license, certificate of registry, or merchant mariner’s document under federal law; (C) a vessel pilot; (D) an individual engaged on a towing vessel that pushes, pulls, or hauls alongside a tank vessel; (E) an individual with access to security sensitive information; and (F) other individuals engaged in port security activities.

Surprisingly, there is no counterpart provision in the proposed TWIC regulations. In the preamble of the NPRM, the TSA summarizes the eligibility provision thus:

Section 102 of the MTSA requires the Secretary of Homeland Security to issue a biometric transportation security credential to merchant mariners “issued a license, certificate of registry, or merchant mariners document” and individuals who require unescorted access to secure areas of vessels and facilities.

A comparison of the two provisions reveals that the summary has omitted some of the statutory categories. The most glaring omission is with regard to an individual with access to security sensitive information. At least some of these individuals may not need unescorted access to the secure area of a vessel or facility in order to perform their work, but the statute directs that the TWIC requirement applies regardless.

The MTSA directs that an individual nominally eligible for a TWIC may not be denied same unless the Secretary determines that the individual:

- (1) has been convicted within the preceding 7-year period of a felony that either the Secretary believes could cause the individual to be a terrorism security risk to the United States or for causing a severe transportation security incident;
- (2) has been released from incarceration within the preceding 5-year period for committing a felony described above;
- (3) may be denied admission to the United States or removed from the United States under the Immigration and Nationality Act; or
- (4) otherwise poses a terrorism security risk to the United States.

The TSA proposes to implement this provision by amending its current regulations relating to security threat assessments for transportation workers who apply for a commercial drivers license (CDL) with a hazardous materials endorsement (HME). With regard to criminal

offenses, the regulations have three categories: (a) permanent disqualifying criminal offenses (such as espionage or treason); (b) interim disqualifying criminal offenses (such as murder, kidnapping, or rape); and (c) persons who are wanted or under indictment for one of the listed felonies. Various labor organizations assert that disqualifying criminal convictions should be limited to those related to espionage or treason.

The NPRM proposes only minor changes to the current immigration status regulation. There is a potential problem, though, with regard to the process used to check the immigration status of TWIC applicants. The NPRM states that TSA will verify an applicant's identity through use of the US Citizenship and Immigration Services (CIS) Employment Eligibility Verification (Form I-9) process. The US Government Accountability Office (GAO) found significant problems with the validity of the data in these government records.

The MTSA provides that information obtained by the Attorney General or the Secretary during the TWIC process may not be made available to the public, including the individual's employer. Research has failed to find a provision in the proposed rulemaking addressing this aspect of the MTSA. A probable reason for the confidentiality provision is to avoid the problems that arose in the 1950's when the Coast Guard's port security card (or Z-Card) program came into effect. Some maritime employers used information obtained through that process as an excuse to fire employees considered to be troublemakers and union organizers. During that period, this information was also utilized to weed out persons with communist sympathies.

In summary, while there are many good points to the TWIC concept, this particular proposal appears to be premature and somewhat excessive. The screening process and the appeal and waiver procedures in particular appear to be more than adequate. There are going to be problems with the physical portion of the TWIC program (cards and card readers) because the technology has yet to be finalized and put into production. TSA missed an opportunity to avoid imposing a burdensome program on a low-risk portion of the maritime industry, but may still be able to recover. Overall, the program is not yet ready for prime time.

The TSA recently announced what will be at least a partial delay and regrouping. On August 21, 2006, it published in the Federal Register a notice stating that facility and vessel owners and operators will not be required to purchase or install card readers during the first phase of the TWIC implementation. The public will be afforded a further opportunity to comment on that aspect of the TWIC program, which has been moved into a separate regulatory project. The initial rulemaking (as modified), though, will provide guidelines for the background check process and issuance of the TWIC card, and may possibly allow TSA to begin issuing the TWIC cards by the end of 2006.

This two-step approach has already engendered criticism. Members of the information technology (IT) community correctly point out that issuing the TWIC cards before the card reader equipment has been built and tested runs a high risk of failure. If things don't work out exactly as planned, the readers and the cards may be incompatible. Since the TWIC program from commencement assumed that the FIPS program would be in place before the TWIC cards

TWIC – a bridge too far

Page 5

September 2006

and readers were put into production, it would be far preferable to delay the TWIC program until the FIPS program has proven the technology. The hiatus would also allow TSA to address other problems in the TWIC program, such as those noted above. An unnecessary rush at this time may provide only the appearance of additional security and, ultimately, may prove to be another case of ‘a bridge too far.’

© Maritime Reporter and Engineering News