MARITIME REPORTER AND ENGINEERING NEWS

Tel 352 692 5493
Fax 352 692 5494

Dennis L. Bryant
Bryant's Maritime Consulting
4845 SW 91st Way
Gainesville, FL 32608-8135

May 2012

The useless TWIC

Dennis L. Bryant

With visions of al Qaeda terrorists lurking on US waterfronts and in the bowls of US-flag vessels, Congress in 2002 included in the Maritime Transportation Security Act (MTSA) a requirement that unescorted access to secure areas in US waterfront facilities and US-flag vessels be limited to individuals who had been properly issued biometric transportation security cards. The laudable goals were to reduce not only the risk of a "transportation security incident", but also the level of crime on the waterfront. Experience has clearly shown that the concept that the issuance of high-tech biometric transportation security cards, called the Transportation Worker Identification Credential or TWIC, could achieve these goals was fatally flawed from the beginning.

Implementation of the TWIC program, which had been assigned to the Transportation Security Administration (TSA) within the Department of Homeland Security (DHS), was delayed for an excessive period. It took several years to decide on what biometric features to utilize in the TWIC and how those features should be encoded. It took another few years to develop the technology to produce the cards and gear up for production. This period included a dust-up regarding the location of the production facility. A contractor was hired to open and man offices nationwide to process applications by individuals seeking TWICs and to issue/activate the TWICs once they had been produced. A glitch occurred when the TSA facility collecting electronic information regarding TWIC applicants suffered a blackout before it had updated its records. Many individuals had to resubmit their applications as a result.

In November 2011, the TSA issued a notice stating that approximately 26,000 TWIC cards issued prior to April 5, 2011 were improperly encoded and may not work with TWIC card readers. Due to a card production system error, the number of characters in the Federal Agency Smart Credential Number (FASC-N) embedded in these defective cards was truncated. The cards will be replaced at no cost to the individual, according to the TSA notice. The TSA elected, though, to not directly notify the individuals with faulty cards. Rather, it posted a list of the affected TWICs and asked all the potentially affected individuals to access and check the list. The TSA also did not discuss the inconvenience and expense that will be incurred by these individuals in returning to the TWIC registration/distribution site to obtain and activate the new TWIC card.

E-mail dennis.l.bryant@gmail.com
Internet http://brymar-consulting.com/

An individual who has reported his or her TWIC as lost, damaged, or stolen is supposed to be provided a replacement card within seven days. Initial policy allowed owners and operators of MTSA-regulated vessels, facilities, and OCS facilities to authorize unescorted access to secure areas to individuals who had made the required report to TSA for up to seven days while awaiting the replacement card. In October 2010, the Coast Guard issued a policy statement to the effect that the owners and operators could authorize unescorted access to such individuals for an additional thirty (30) days because of a backlog at TSA in the issuance of replacement TWIC cards. That policy remains in effect.

Also in October 2010, the Coast Guard issued a Marine Safety Information Bulletin stating that it has received reports of malfunctioning internal antennas on some TWIC cards. The affected cards are functionally unrecognizable to contactless TWIC readers, but should still work with contact readers. The cards are also valid for access based on visual inspection. The bulletin recommended that the individual with such a TWIC card contact TSA for a replacement and noted that the cost of replacement is $60.00. No mention was made in the bulletin as to whether the cause of the defective internal antenna was due to the production process or due to rough handling by the individual card holder.

The card stock used for the TWIC was found to be insufficiently durable for the marine environment and typical maritime working conditions. As a result, an unexpectedly high number of cards malfunctioned electronically and could not be read by the electronic readers.

Rumor has it that counterfeit TWIC cards are available for purchase on the black market at a cost of approximately $100 each. In May 2010, the Coast Guard issued a Maritime Safety & Security Bulletin acknowledging the presence of fraudulent TWIC cards and advising security officers and individuals with security duties to be vigilant and to closely follow security procedures when granting unescorted access to MTSA-regulated secure areas. In 2009, an illegal alien was sentenced to eight months in prison after pleading guilty to unlawful transfer of two fraudulent TWIC cards. In 2011, undercover GAO investigators obtained fraudulent TWIC cards and were able to drive a vehicle containing simulated explosive material into a secure area at a waterfront facility. This led Representative John Mica (R-FL), Chairman of the House Committee on Transportation and Infrastructure, to state that the TWICs were “at best no more useful than library cards.”

The TWIC, when issued, included a photograph of the individual and the embedded biometric information. Currently, the individual presents the TWIC card to a security guard. If the card looks legitimate and the individual looks like the photograph, entry to the secure area is generally accorded. Plans call for each entry point at facility and vessel secure areas eventually to be equipped with electronic card readers, similar to the ubiquitous ATM card terminals. Individuals would swipe their TWICs (or hold it in close proximity, if a contactless reader was installed) and match the biometric information (fingerprints) to gain access. Fixed card readers are still being tested. Development of portable wireless card readers is several years away, at the earliest.

The Department of Homeland Security (DHS) recently completed a pilot program to evaluate electronic TWIC card readers. DHS concluded that the TWIC reader systems function properly when they are designed, installed, and operated in a manner consistent with the characteristics and business needs of the facility or vessel operation. Important caveats were attached to this declaration of success. A number of operational and technological difficulties were documented during the pilot program. Reader performance varied widely during the pilot. The time and effort required to install electronic readers and reader infrastructure varied widely among pilot participants. Extensive training was necessary for personnel operating the electronic reader system and some training was required for individual card holders. Some readers experienced difficulty scanning fingerprints of the individual, particularly during inclement weather. One of the findings of the pilot program, not surprisingly, was that the conditions under which TWIC readers had to perform were significantly more challenging than those commonly found at office locations.

In May 2011, the Government Accountability Office (GAO) issued a report stating, in pertinent part, that the DHS has not assessed the TWIC program's effectiveness at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned, is more effective than prior approaches used to limit access to ports and facilities. The DHS has not completed a risk-informed cost-benefit analysis that considers existing security risks and it has not completed a regulatory analysis for its upcoming regulation on using TWICs with card readers.

Issues regarding the TWIC program are numerous. The TWIC cards are not securely produced. Quality control during the production process is lacking. The cards are not substantial enough to stand up to normal handling. They are easy to counterfeit. The electronic card readers only work, if at all, after much time, expensive, and training of both the security staff and the card holders.

This litany of problems has eroded industry's faith in the TWIC program. The TWIC card, as things now stand, is little more than a glorified and very expensive flash pass. The process has made it difficult for individuals in the maritime industry to obtain a legitimate TWIC card, while unauthorized persons can obtain a fraudulent card for about $100. Under the current program, the biometric transportation security card decreed by Congress in the heat of the moment following the horrific terrorist attacks on September 11, 2001 – the TWIC card – is virtually useless.