

EQUIPMENT

TWIC

PRESENT VALUE? – THE IMPACT OF TECHNOLOGY

By: *Martin Pilsch, Equipment & Port Development*

Since February 3, 2008, I have carried my TWIC. From the time it was activated to the actual TWIC rollout, however, my credential remained in my pocket. I never used it. My driver's license and a call for an appointment got me in to every marine terminal I visited.

My travels took me to numerous ports along the U.S. East Coast. As TWIC rollout loomed, I would see notifications of the impending event on electronic billboards and signs at every port security check point. I would receive written notices along with my temporary pass as I went through the gate. The billboards, signs and notifications said, "No TWIC, No Entry." My TWIC was still in my pocket.

I was excited though. For once in my life, I was prepared. Finally, my \$132.50 investment was going to pay off and as TWIC did roll out at each group of ports, I continued my visits, this time with TWIC at the ready. At least, it had come out of my pocket.

During the early period, however, the TWIC deadline at many ports had not been reached. My drivers license continued as my primary form of identification. At ports where rollout had been implemented, it was still my drivers license that was the key to opening the door even though I handed my TWIC to the security guard. Ports in the rollout groups were required to look at the TWIC but didn't know what to do with it. Truth be known, there wasn't much they could do. At this time, the value of the TWIC is limited to the picture on it.

As most of us know by now, TWIC consists of two critical components, the actual credential carried by the worker and the credential reader used by the facility owners to control access. The value of the TWIC is not the visual elements, but based upon smart card technology embedded into it.

On the card itself is a picture of the holder, the name of the holder, and the card's expiration date. The smart card portion of the credential consists of a small, integrated gold circuit chip housing data, a linear bar code and a magnetic stripe. All of these technologies are capable of instantly gathering the holder's personal background data. The complete package is a bit more than 4" long and 2 ½" wide including a plastic holder.

Even with TWIC's complicated past, the explanation of its present status is fairly simple. For true security value, rollout was premature. With all of the technology that comes with it, today, the credential has less value than a toll transponder. At this point, however, the toll transponder is one up on TWIC. It can be read.

To give the architects of the program some credit, the rollout does have some redeeming value. One, it signifies major success in the effort to get TWIC out to qualified constituents. A number of problems for those who have had their applications refused, remain however. Two, rolling out the TWIC gets people use to carrying it.

The truly effective implementation of TWIC is tied to the development of a TWIC reader and the implementation and eventual use of a reader is somewhere out on a horizon, yet to be defined. The edict, "No TWIC, No Entry," is in effect, but for effective identification, it is business as usual.

Impeding unauthorized access is the name of the game for seaport security. This effort can take many forms and implementation has its costs. The federal maritime security program forces seaports to make investments that while necessary to control access, also comply with Federal regulations. The program is often looked upon by local entities as an additional, un-recoupable burden on an already strained financial system. With little fanfare and minimal financial support, however, ports and marine terminals began the task, increasing police forces, engaging security services, improving physical barriers, purchasing surveillance systems, developing access technology and identifying and checking everyone who desires entrance to their terminals.

There are three important elements tied to the use of TWIC as an effective tool for secure port access. Two are extensions of smart technology with federal implementation plans for each, thrown in. The third, keys on the other two, establishing local access procedures. The first element is the development of the TWIC, Transportation Worker's Identification Credential. The industry has chosen a smart card designed to identify its holder by photo and biometrics stored on a national database. The second element is the TWIC reader, incorporating technology capable of reading the card, confirming that the data stored on it is valid. The combination of the credential and the reader provides the port's security force assurance that the holder is who the credential says he is, that the credential is verified and that the credential is valid.

The third element is the individual port plan, or Facility Security Plan (FSP). The plans are formulated by each port and establish the security procedures by which each port will operate. Experience confirms that each port's plan has its differences. These plans were initially established by port marine terminals as their overall programs matured prior to TWIC. Ultimately, they will depend upon the activation of the TWIC card and the implementation of TWIC readers. As these come about, plans will require an adjustment. True application of TWIC brings on many new issues. How to bring the card and the reader together to realize reliable secure access, how to effectively use TWIC without impeding commerce and what to do if the reader reacts to a negative scan, are but a few.

To bring some order to their Facility Security Plans, ports have had to designate secure and unsecured areas relative to their facilities. The designation of " a secure area" indicates that it is critical to the operation of the port and that a successful terrorist attack would be devastating. Control of access to a secure area is a priority.

Ports have also had to define the ability of individuals to enter their secure areas unescorted. Considerations on how to handle employees, vendors, support personnel, touring groups and foreign visitors are but a few of the issues. By definition, holding the federally issued TWIC allows you unescorted access. Individual Facility Security Plans (FSPs), however, define designated secure areas and control unescorted access. Quite simply, you must have a TWIC to enter a secure area. The possession of a TWIC, however, does not authorize your access.

Within each Port's FSP, true control depends heavily on a completely developed application of the TWIC program. This means receiving the TWIC from personnel desiring access, scanning it and reading the information contained on it.

TWIC is a program that despite all of its hiccups and lingering requirements to clear numerous obstacles, should work. What has happened, however, is that after almost three years, the TWIC program has not been able to deliver the full package. TWIC cards cannot be read and therefore they truly make no positive impact on port security at this time.

Despite all of this and the fact that the TWIC program continues to drag out, I have learned to accept the realities. The first is that the national database has been created and my life history is floating somewhere in cyber space. Second is that the issuance and rollout of TWIC is about to be completed, but no one can really use it. Third is that TWIC's true value to national port security will

be delayed indefinitely while we search for reader technology and rules to govern its use. Fourth is that the information stored on the TWIC and the database should be accessible at virtually all access points to marine terminals around the country, but, they are not. Fifth is that when the readers do appear and all the work has been completed, the value of the TWIC will depend upon the data and the attention of the individual who is checking it, ensuring that what the reader reports is valid. Sixth is the hope that after all of this time, TWIC background checks do not become outdated. A person can change a lifetime in a very short period.

The final reality is that just like many others, I paid my dues, in all respects, and by the time I see my TWIC actually scanned, my data read and my access to a marine terminal approved, my card will be over three years old - presuming I don't lose it. I will have only two more years left to see it open the gates before I'll have to report in for a renewal. This is of course assuming that the TWIC program will be completed by then.

I am also assuming that I will renew, as long as age hasn't forced me into retirement or I am still alive. In either case, I am taking my TWIC with me. If I have it with me when I pass, perhaps Saint Peter can read it for me? The actual reality is, however, that the devil will probably have to do it. Do you think he cares?