

NAWE members are very concerned about the direction the NMSAC TWIC Working Group appears to be taking regarding technology. (draft #1 ... 1/18/07)

Background:

NAWE applauds the involvement of NMSAC in helping to define operational requirements and technological specifications for the underlying technology for TWIC readers. The dialogue amongst maritime and biometric technology representatives has been informative. But as the discussion evolves into greater details about what technology is appropriate and suitable, we seem to be losing sight of the “big picture”. We must constantly remind ourselves that the technology that is ultimately adopted must apply to hundreds of thousands of cards and cardholders, thousands of readers, and hundreds of different environments and circumstances. Furthermore, the system must work day 24 hours a day and 7 days a week often under great operational pressure for speed and efficiency.

NAWE members, through experience, understand how a minor glitch in the logistics chain can expand into a system-wide collapse that can bring the national economy to its knees. We must make sure that the TWIC system is manageable by the large and sophisticated terminal operators as well as the small operators that will view the program as highly burdensome. We must understand the broad spectrum of people that will use the TWIC card ranging from a company “IT guru” to a contract worker that might need access to a secure area for janitorial services. As we reflect back on the initial meetings of the working group, we failed to identify arguably the most important “guiding principle” of all, the necessity to keep the system “*as simple as reasonably possible*”

How to Keep TWIC System Simple:

There are numerous facets of the TWIC system that might be reviewed to determine if a simpler and effective approach should be adopted. NAWA wishes to focus on only one possible opportunity ... to avoid the use of encryption to secure data transmission. We believe the benefits associated with encryption are far outweighed by the cost and increase in complexity. We believe the increased complexity will translate into exponentially more problems and breakdowns. We need to keep the system simple.

Assessment of Cost/Benefit of Encryption:

It is difficult to understand the benefits of encryption for the intended application. What is the information we want to keep secure? It is our understanding that all private and confidential information about an individual gathered during enrollment and background check will be retained by TSA in their central data bank. In essence, the card will have a photo, a CHUID, and the individual’s biometric fingerprint template. Disregarding the notion that one could easily compromise someone’s fingerprint on a beer can, we have been advised that it is almost impossible to recreate a finger print from a template. Therefore, even if a template were stolen during the contactless transmission of data from card to reader, it is difficult to understand how the thief can use that template. They would have to replicate the corresponding fingerprint, and somehow find a way to present it at the reader. Anything

is possible but this scenario seems highly unlikely. So what is the benefit of encryption? We do not challenge the notion that encryption would make it more difficult for the data to be compromised during transmission. However, it seems evident to us that by using the CHUID and biometric finger print template, there is significant security and privacy already built into the system. The benefit of encryption can only be measured by the “incremental increase” in security and privacy above and beyond what is already built-in by the use of CHUID and templates. There is probably no standard of measure to define this incremental increase, but the members of NAWE sense that it is relatively small.

On the other hand, let’s look at the possible cost of incorporating encryption. Each transaction will require encryption and decryption which will require time and another opportunity for something to go wrong. We’ve been advised that before encryption and decryption, there would have to be some form of authentication or handshake to make sure that the card and reader verify that each is authorized to read the other’s data. Furthermore, in order for authentication to work, some form of key management has to be put in place. To make matters even worse, if a key is compromised, every reader in that “key community” would have to be adjusted for a new key. It’s unclear whether or not something has to be done with the cards in that key community. But the bottom line is that encryption brings with it a host of additional challenges and complications.

Summary:

NAWE remains fully supportive of the TWIC program. We’re pleased and encouraged that Phase I of TWIC will be rolling out soon. We believe the bulk of the security benefits from TWIC are in the screening and background checks. Some members believe that as much as 70% of the benefits of the total program are in Phase I. Nevertheless, we recognize that the program is not complete without Phase II. But we’re very concerned that the NMSAC Working Group appears to be leaning towards unnecessarily increasing data security and privacy and making the TWIC system dangerously too complicated. We must recognize the dangers of making the system overly complex. We must keep the system as simple as possible while protecting the privacy of individuals and the security of the system. This can be achieved without resorting to the complexities of encryption.