

**NMSAC TWIC Working Group**  
**Open/New Items**  
**a/o 1/10/07**

Following is a summary of other comments/issues beyond the original IBIA document that have been presented for the working group's consideration. We encourage TWG to comment on these items.

A. In the original list of questions submitted for the working group's consideration, the IBIA suggested we develop a series of high-level use case scenarios (question #2), outline the divergence between FIPS 201 (question #3), and develop a draft TWIC data model (question #4). Because of the diversity of port, vessel and off-shore operations, we determined that it is not practical for us to respond to #2, and we also elected not to respond to #3; both of these have been addressed generally through the course of our working group discussions. However, #3 remains unaddressed. Does the maritime group want to respond? Does the security group need a response?

3. TWIC Card Data Model

To the extent practical, TSA should describe its draft concept of a TWIC card data model. NMSAC should make recommendations for any changes or additions to this data model that are needed to support operational requirements.

B. We should focus on the "incremental" changes required to FIPS 201 to meet TWIC needs. A minor change (though perhaps a major change in policy) to FIPS 201 might encourage greater vendor participation and lower prices for TWIC applications. Alternatively, a minor change might be embraced by NIST in a Special Publication to support TWIC.

One possible advantage to assimilating TWIC under the NIST umbrella is that the same GSA Approved Product List and process can be used rather than standing up a separate TWIC approval testing laboratory.

C. Specifications for a new and unique TWIC card will take man years. Development will also take a long time.

D. We are approaching this incorrectly. Rather than develop a reader spec first with policy decisions to follow, it makes more sense to first resolve the policy questions and then incorporate technology to support them. Among the most significant of these are the requirement for TWIC readers on vessels (ref. specifically OSMA concerns), international considerations (MMP and others), the inability to lab test and field test the cards prior to the implementation of the pilot program required by the SAFE Port Act (several) , etc.

E. In follow up to his discussion during the 12/20 conference call, Dr. John Campbell offers the following:

The ILO went through a lot of the same struggles of balancing cost, security and convenience when it developed the Seafarers' Identity Document as the US is now experiencing around TWIC. In both cases, the needs of workers, employers/facility owners and government were not necessarily aligned and had to be balanced. Unfortunately, ILO did not have any unbiased source of external advice and ended up choosing compromises that have caused issues in the deployment of the SID. We should work to ensure that TWIC does not experience the same problems, with an initial solution being rushed through because of pressure on TSA, and later turning out once it is implemented to have hidden problems.

As an example, consider the issue of data storage on a chip and the encryption that should be used to protect that data. The ePassport solution is to have data printed on the document that must be optically read before the chip can be unlocked. This makes it almost impossible to initiate communication with the ePassport and thus read the data from it unless the owner of the ePassport has voluntarily surrendered it for optical reading. Of course, there is still the possibility of interception once communication has begun, and this is why full encryption schemes are being recommended for fingerprints on an ePassport. The ILO SID goes even further. It has no chip and the fingerprint data must be read from a two dimensional barcode, which can't be read until the seafarer has surrendered their document and also can't be snooped or intercepted. Of course, if the barcode becomes worn or damaged, so it can't be read, the SID has a problem. Similarly, if a TWIC is bent such that the antenna breaks or the chip is damaged, it becomes useless. Ultimately, a better solution for both would be to have the relevant information stored in both a chip and a 2D barcode. This would allow for the possibility of a full encryption scheme where it is required for contactless chips, but for a small port, a single pier, or the gangplank of a single vessel, a simple hand held reader would work, and that reader could either read the chip using whatever encryption scheme is defined, or read the fingerprint template from the barcode and not have to worry about encryption. There would also be an immediate backup solution for verification of the fingerprint, if either the barcode or chip was damaged, since the fingerprints would be encoded twice on each document.

This solution allows more flexibility for all the end users of the system, and hopefully will be the solution for the next generation ILO SID. It would benefit end users of the TWIC, and hopefully the TWIC will be compatible with the next generation SID, which will save time and money for a large segment of the TWIC card holder population. Since TWIC is designed for a maritime environment, with much harsher conditions than those experienced in the majority of FIPS 201 PIV deployments, it is important that the unique requirements of this environment be reflected in the final solution for the TWIC.