TESTIMONY

before the

U.S. House of Representatives
Committee on Homeland Security

Hearing on

Homeland Security Failures: TWIC Examined

by

Lisa B. Himber
Vice President

Maritime Exchange For The
Delaware River And Bay

October 31, 2007

Testimony of Lisa B. Himber
October 18, 2007

Good Morning Mr. Chairman, Congressman King, and members of the Committee, and thank you for the opportunity to testify on the importance of the Transportation Worker Identification Credential (TWIC) program. My name is Lisa Himber, and I am Vice President of the Maritime Exchange for the Delaware River and Bay, a non-profit trade association representing the Delaware Valley port community. I am also a member of the National Maritime Security Advisory Committee (NMSAC) and have chaired its TWIC working group since the committee's inception in March of 2005.

Having been involved with the program since February of 2002, my organization and its members are all too keenly aware of the massive challenges facing our ports as we seek to implement the TWIC related provisions of the Maritime Transportation Security the Security and Accountability for Every Port Acts. We appreciate this Committee's understanding of this important program and its efforts toward keeping TWIC in the public spotlight.

Congress and the Department of Homeland Security (DHS) have created any number of programs since the events of 9/11 forced us to re-examine our approach to border security. MTSA required security plans which have hardened our vessels and facilities, and the Trade Act and Bioterrorism Acts of 2002 spawned programs such as the 24-hour advance cargo manifest rule and advance electronic notice of food imports, which have provided greater visibility into the cargo supply chain. And while both the maritime industry and the government agencies which regulate it were forced to make radical changes in their business processes to successfully implement these far-reaching programs, none of these so dramatically changed the landscape as TWIC has the potential to do. With the implementation of the TWIC program, we will begin to focus on that last component of maritime security: the people who work on our vessels and piers.

Our industry has long supported the TWIC concept, and we have continued to demonstrate that support over the last five years. Undoubtedly, it has been a long and hard road to get us to where we are today, and as we stand on the brink of bringing the program from the pilot stage to a full production environment, it is paramount that we learn from the mistakes of the past and take all conceivable steps to ensure the program is implemented in such a way as to meet all its stated goals.

We fully understand the difficulties Transportation Security Administration is facing as it seeks to deploy a program of this complexity and magnitude. And it is our sincere hope that the agency will not only listen to the concerns of its stakeholders – those very people who have the most to gain from a more secure maritime environment – but that they will act on the recommendations of the many maritime professionals who have dedicated their time, resources, and expertise to making this program a success.

So while we look forward to working with TSA and its contractors to resolve the unexpected bumps in the road we are certain to encounter, we believe it is appropriate to highlight those concerns that, if not addressed, may unnecessarily impede our progress.

I will focus my comments today in two key areas. The Phase I/Card Issuance and Phase II/Reader Deployment.

PHASE I/CARD ISSUANCE

Let me begin by saying that since the October startup in Wilmington, Delaware, the initial TWIC deployment appears to be going fairly well. Though there have been a few minor complications, these were not unexpected, and we remain confident that TSA and its contractors will quickly resolve issues as they arise. One issue which has surfaced as having the potential to cause significant problems relates to the capture and verification of the biometric, which I will discuss shortly.

That being said, there are several specific areas which we believe need further attention.

Communication – Throughout the pilot program, both Congress maritime stakeholders expressed their belief that TSA had done a poor job of communicating information and project status. We were pleased when TSA and Lockheed Martin announced the formation of a TWIC Stakeholder Communication Committee which would serve as a forum for TWIC managers to provide information and obtain industry feedback. The Committee has met many times since its formation last spring, yet unfortunately it has not served its purpose. For example, when TSA announced it would not start program rollout in March as planned, stakeholders were not provided with information as to the cause of the delay or provided with updates over the intervening months.

We do not understand why information such as the deployment schedule, enrollment center locations, and other important information concerning the TWIC rollout must remain a secret from those who will be affected by decisions TSA makes. As the agency should have learned, failure to provide timely and relevant information only leads to speculation, poor planning, and an overall inability for stakeholders to help TSA achieve success.

In addition, many port operators and others remain concerned that many truck drivers and other workers are largely unaware of the requirement. We acknowledge that TSA and its contractors have worked to broaden outreach and awareness efforts, but it appears more needs to be done in this area.

The Enrollment Process – For reasons which were never made entirely clear, the third phase of the TWIC pilot program, which was designed to test the business processes of applying for, obtaining, and using the TWIC, was severely abbreviated. In addition to issuing only a limited number of cards, only about 2,000 cards were produced in the East Coast Pilot program, very few of the actual processes to be followed to obtain a TWIC were tested in the field. Most of these related to the use of the card readers, however neither were several of the enrollment and card issuance processes fully examined.

Having been through the process, I can attest to the fact that, while it could be streamlined somewhat, overall the experience was not overly burdensome. I applied for my card on Monday, October 15, and received notification that my card was available for pick up within five days. The pre-enrollment, enrollment and card activation processes were fairly simple and took only about 45 minutes in total.

Impact on the Workforce – Foremost among the open questions relates to the lack of a background check for the volunteer pilot program participants. We were told that TSA did not have the regulatory authority to conduct a background check during the pilot program; as a result no empirical data are available to determine what, if any, impact this program will have on the workforce. What we do know is that there are maritime workers who have disqualifying criminal offenses in their backgrounds, yet we do not know their numbers or whether those workers will be able to obtain the necessary waivers.

We are heartened by the statistics provided by TSA regarding the number of individuals who have successfully applied for waivers in the Hazardous Materials endorsement program. Yet we are concerned that TSA has indicated that the majority of people who were initially disqualified from receiving a Hazmat endorsement did not apply for waivers. Whether this is because they were unaware of the opportunity, intimidated by or unable to understand the process, or felt they would not be eligible is unknown. It is clear, however, that TSA must do all it can to help these individuals through the process. No one wants to see a qualified maritime worker deprived of his or her livelihood.

The Casual Worker – Over the last five years, there has been a great deal of concern and discussion surrounding how ports and vessels will accommodate the need to hire casual workers to process cargoes during peak operating times. While the regulation allows for workers without TWICs to enter under escort, a practical method to implement an escort program has yet to be developed.

First, there are safety concerns that must be addressed to effectively implement an escort program. Certainly, a worker cannot effectively monitor both his own work and the activities of others. In addition, the physical layout of the facility or type of cargo being moved (such as automobiles, which are driven onto the port) may prevent the implementation of an escort policy. It is certainly easy enough to stipulate as policy that all workers must have TWICs – until there is a shortage of eligible workers and cargo does not move.

Some believe ports should be allowed to create a program to grandfather casual workers if they so choose. For example, eligibility could be restricted to individuals who have a history of working at a given port, and a ceiling set on number of hours worked prior to requiring a TWIC. Facilities could be given the option to create a "temporary" credential or visitor's pass in lieu of requiring escorts. If appropriate, when the individual's identification documentation is validated, his photograph could be taken and other information entered into the facility access control system. If necessary, this information could be submitted to DHS for recordkeeping purposes.

While some believe this would circumvent the TWIC process, and certainly such concerns are legitimate, allowing a program of this nature in the short term would ensure a more smooth transition to the new requirements. The ultimate outcome of TWIC, for better or worse, will be a change in maritime industry hiring practices. We must take advantage of the opportunity TWIC will afford to "professionalize" the workforce, as we anticipate that various trade and other unions will develop a cadre of members "certified" to work on regulated areas. At the same time, however, it is necessary that we take measures to ensure commerce can continue to flow smoothly in the interim.

Use of Biometrics – The prototype did not test use of biometrics with workers at port facilities. This is a significant concern as there is no evidence that the fingerprint will suffice as a biometric in a maritime environment. Although the potential adverse impact is less severe than it will be after use of card readers is phased in, there are still unanswered policy questions. For example, how will TSA issue a credential to an individual whose biometric cannot be captured? What will be used for verification of such individual during a random spot check by the Coast Guard?

Of the 16 people who applied for their TWICs at Wilmington on Monday October 15, at least three of those encountered problems in activating the cards because the biometric verification failed. This is an alarmingly high percentage and could point to a significant flaw in the system that must be contained before the program is expanded. It is important to note that this was in an office environment where conditions are fairly clean and could be more problematic in a weather-exposed port or vessel environment.

This is particularly puzzling since each enrollee was able to successfully scan their two index fingers immediately after enrollment of their ten fingerprints. As a result of the initial problems observed during card activation, I am concerned that there could be a technical issue with the method used by the contractor for generating the fingerprint data stored on the TWIC card and how that data is being verified at activation. We hope that TSA will investigate this matter and take corrective action before they issue a significant volume of TWIC cards that might result in excessive biometric verification failures for legitimate card holders.

Phase-In Schedule – When the final TWIC rulemaking was promulgated in January of this year, TSA anticipated a late March startup and mandated that initial rollout must be completed by September of 2008, an 18-month schedule we believed was ambitious at the outset. Yet enrollment did not begin until October, leaving only an 11-month window to complete the initial enrollment process. While we applaud TSA's desire to complete the process quickly based on the original schedule, we do not believe this timetable is realistic and suggest consideration be given to planning for an extension. Without proper planning, making the decision at a later date could create real problems for both the contractors and for maritime workers.

In addition, we recommend that TSA and Coast Guard begin compliance at all ports simultaneously. First, staggering TWIC compliance dates can cause competitive disadvantages for those areas which have earlier dates – as can any program which makes it more difficult, costly or cumbersome to move cargo through one port over another. In addition, because the maritime worker population is largely mobile, it will be difficult for the ports where TWIC has been declared mandatory to escort mariners, or truck drivers arriving from areas where TWIC is not yet available or mandatory.

In any event, it is crucial that there is concurrence between the Captains of the Port and and key port stakeholders when the decision is made to begin to enforce compliance in any given region.

Enrollment Center Locations – A sufficient number and convenient locations of TWIC enrollment centers will be critical to successful program deployment. While TSA has guaranteed there will be enrollment sites in at least 140 port cities, we have yet to learn the number of locations within those ports, nor how long they those sites will be operational. Further, we have not been provided with any information on the locations of centers beyond September of 2008.

Decisions on locations of enrollment centers beyond the initial rollout should not be left to the contractor's discretion but must be a cooperative agreement between TSA and the maritime community to facilitate the TWIC enrollment and card replacement processes.

Further, the enrollment process is not geared toward mobile populations, particularly truck drivers. The program is designed in such a way that individuals must retrieve their TWICs after production at the same location as they applied. Many drivers arrive at Delaware River ports from other parts of the country. Until the program is fully implemented, these drivers will not have their TWIC cards. With the sheer volume of trucks moving through facility gates every day, it is not feasible that facilities, importers, or others could provide resources to escort these individuals.

Trusted Agents – Because of the sensitive nature of the data these individuals have access to, we have suggested that TWIC trusted agents be subject to higher scrutiny than TWIC applicants. In addition to undergoing the same threat assessment procedure as a potential TWIC holder, we have recommended that trusted agents also be subject to financial history and other relevant background checks. To date, we have not received any assurances in this regard.

Based on our experience during the pilot program, we also recommended that trusted agents receive relevant customer service and "business" training, such as how to appropriately swipe a credit card, as well as comport themselves in a professional manner. The Trusted Agents I have encountered in Wilmington have certainly been friendly and polite. However, when I arrived at the enrollment center after completing the pre-enrollment process, the Trusted Agent could not access my information. As it turned out, there was not a system problem, but rather it was a training issue with that particular Agent. Further, when I went to retrieve my card, there was a lengthy process while information was uploaded from the system to the card. The Agent was unable to answer my questions regarding what information was being encoded into the card.

Needless to say, it is critical that Trusted Agents receive thorough training on the TWIC program itself. While we recognize that it is still early in the process, given that the Trusted Agents have been onsite and undergoing training in Wilmington for several months, we are extremely concerned to hear that there are training problems right out of the gate. If indeed the population estimate of 750,000 workers is as understated as many port officials believe, and Lockheed Martin is compelled to quickly fill Trusted Agent positions to accommodate a greater than anticipated demand, how will these issues be handled?

Applying for an obtaining TWICs will take time and will cost, in some cases, a great deal of money. It is incumbent upon TSA to ensure these issues are anticipated and addressed.

Use of Readers During Phase I – The TWIC regulations require that individuals seeking unescorted access to a restricted area present their cards for visual inspection. Many facilities have invested in electronic card readers which allow access through automated gates. In addition to the increased throughput time and personnel costs associated with visually inspecting each card, many believe that eliminating the electronic read in favor of the human review is in fact taking a step backwards in terms of security.

The TWIC cards being issued today are machine readable. We have suggested to TSA and Coast Guard that the visual inspection should be considered a minimum standard; vessels and facilities should have the option to exceed that standard by using TWIC readers for access during Phase I, even though readers are not yet required.

Lost or Stolen Credentials – We appreciate that TSA has provided a mechanism to accommodate access for workers whose cards may have been lost or stolen. Yet this mechanism is only available to direct employees of a facility or vessel, and it should be made available to all credentialed workers. Further, the process to verify/enforce this provision is unclear. While the request for a replacement card can be made on-line, ostensibly eliminating the need to make two trips to the enrollment center, the guidance provided stipulates that proof during the 7-day grace period must be provided in the form of a receipt, which can only be obtained by visiting the enrollment center. Further, since TSA cannot guarantee that a replacement card will be issued in the 7-day time frame, we suggest the guidance be modified to allow for a 30-day grace period.

These are just a few of the outstanding concerns related to the TWIC issuance process. Others include questions about liability – to the vessel or facility operator, to a TWIC holding escort, to companies whose employees may be injured while en route to or from an enrollment center – to a lack of "batch enrollment" capability – to concerns about protecting the data collected and stored during enrollment – to the lack of integration between TWIC and merchant mariner and other existing credentials – or questions surrounding access for law enforcement or emergency personnel.

There are a similar number of open issues and questions surrounding the use of card readers when Phase II of the program begins.

PHASE II/READER DEPLOYMENT

Most maritime professionals applauded the TSA and Coast Guard decision to segregate the rulemaking processes related to card issuance and reader usage. Taken separately, each of these components of the TWIC program is extremely intricate and creates multiple possibilities to unduly hamper maritime operations if not implemented in a thoughtful and deliberate manner. We appreciate that DHS is allowing sufficient time to address the challenges of card issuance prior to introducing the reader component. This is particularly relevant given that many of the critical technologies, such as communication with the central database, use of biometric readers, or using the "hotlist" were not tested, or were tested insufficiently, during the original TWIC pilot program.

We are pleased that DHS, as required by the SafePort Act, will conduct a separate TWIC pilot program to test reader technology and processes. It is our understanding that Coast Guard will publish a proposed rule prior to commencement of the pilot program, and we appreciate the opportunity to provide early comment. And while we recognize that TSA and Coast Guard must complete their planning well in advance of pilot startup, policy decisions must be made prior to choosing technology solutions to be tested. Further it is absolutely crucial that policy decisions are made in concert with maritime stakeholders and that the maritime industry has a voice in the design and development of the pilot program – particularly those ports and vessels who will be participating.

At this point there are two primary concerns technology to be used. The first involves the encryption of the biometric as it is validated during an access request.

Contactless Biometric Read –The Notice of Proposed Rulemaking published in May of 2006 regarding reader usage dictated that contact cards would be used in the TWIC program. Requiring that a card be swiped at a TWIC reader would not only significantly delay maritime operations, but contact readers are more susceptible to failure and present an easy and attractive target to vandals. In response to stakeholder comments, DHS agreed to utilize a contactless card and asked the National Maritime Security Advisory Committee to develop recommendations for a contactless reader specification which could be used at ports and on vessels.

The NMSAC completed its work in February of 2007, and in September DHS published the technical specification for the reader it selected. Despite the fact that the recommendation of its advisory committee, which was supported by a large majority of the comments to the public docket, that the fingerprint template not be encrypted, DHS elected to require such encryption. This is one of the single most important issues DHS will have to address as it enters the second phase of the TWIC rulemaking process.

A. Privacy and Security Considerations – We support the inclusion of measures to protect individual privacy and acknowledge that this prerequisite is as critical to the success of TWIC as are the need to enhance commerce and improve transportation security. It is our understanding that all personally identifiable information about an individual gathered during enrollment will be retained by TSA in its central data bank. The card itself is expected to show and/or contain a photo, a unique cardholder identification number, and the individual's biometric fingerprint template only.

In its design, TSA wisely elected to utilize the fingerprint template rather than a full fingerprint image specifically to address both privacy and operational efficiency concerns. Since only a fingerprint template will be passed between the card and the TWIC reader, the information cannot be reverse-engineered to a full fingerprint image.

Even if the template were "stolen" during contactless transmission to a TWIC reader, and even if somehow it could be used to replicate the original fingerprint, for which we understand no technology currently exists, the "thief" would not be able to use this illegal TWIC as the fingerprint image would not match his own when presented to a biometric reader in conjunction with a TWIC. In addition, an individual interested in "stealing" a fingerprint would meet much less technical resistance and obtain a more accurate representation by lifting it from an object in a public place such as a car door, window or drinking glass.

B. Operational Considerations – There are several concerns with encrypting the fingerprint template. First, every transaction will require encryption and decryption, each of which takes time and affords an opportunity for problems to arise. In addition, prior to encryption and decryption, some form of authentication or "handshake" between the card and reader is necessary to validate that the transaction about to take place is legitimate. In order for such authentication to take place, some form of key management must be in place. Thus, if a key is compromised at one instance, it affects every reader in that "key community."

In summary,

- Adding encryption generally makes the TWIC system more complex and therefore more difficult to develop, use, manage, and maintain.

- Adding encryption will slow processing time to read cards at vessels/facilities.
- The use of keys places an administrative burden and certain liabilities (e.g., responsibility to ensure the key is not compromised) on those charged with key management. Vessel and facility operators are neither prepared nor able to accept these responsibilities.
- Adding encryption will increase TWIC costs.

The NMSAC TWIC Working Group closely studied the issue and as a group concluded that the operational complexities increase by a level of magnitude and to the point where they are not proportionate with any perceived benefit of encrypting the biometric template. In short, there is no empirical evidence that encrypting the fingerprint template affords any additional protection of personal privacy. Despite this, TSA plans to require that the template be encrypted.

This is an area where industry and government are clearly not in agreement. Prior to finalizing this policy decision, TSA and Coast Guard should revisit this issue with industry stakeholders to determine a mutually acceptable solution.

Use of the "Hot List" – To date, TSA has not provided any information on the hotlist to port and vessel operators. Several questions, such as what data will be provided, file transfer protocols, frequency of updates, and method of system query should be discussed well in advance of the pilot program start up.

Reader Manufacturing – One of my members is a manufacturer of card readers and shared the following concerns. "Meeting policy requirements and TWIC technical reader requirements as published means manufacturers and integrators must create a custom product; there is no off the shelf product that meets the control requirements, environmental requirements and system requirements specified. As a result:

a. Manufacturers and integrators have to evaluate the Return on Investment that can be predicted for expending engineering and manufacturing resources to rework existing products to meet the requirements as stated. The fact is that most manufacturing plants require sales in the amounts of 50,000 or more to cost justify the re-engineering and re-tooling effort. There are no guarantees that purchases made by maritime operators and the Coast Guard will reach these volumes, thus cost justifying the customization of product to meet the specified TWIC requirements.

b. The Personal Identity Verification requirements and the TWIC policies continue to be modified, posing additional challenges to engineering efforts both on the software side and the firmware side to meet the TWIC control requirements."

The concern for the maritime industry is of course that readers will be difficult to obtain, and those which may be available will be priced unnecessarily high such that manufacturers can recoup their engineering costs.

There are several other outstanding questions and concerns surrounding the selection and use of card reader technology. These include where readers will be required (e.g., on all vessels or just those meeting certain criteria), the use of a PIN during the TWIC verification procedures, integration with legacy access control systems, whether positive access control will be required, and future expansion of the card.

These are all important issues and it is unclear how DHS plans to work with stakeholders to address them in advance of and during the pilot program.

CONCLUSION

Several years from now, obtaining a TWIC will be standard operating procedure, and its issuance and use will be a matter of routine. But it is clear the next few years will be challenging ones. Now that the process is underway, successful implementation will be dependent on a great deal of communication, understanding, and patience. There is a lot yet to be done, and we must work together to address the many outstanding issues.

Over the years, the maritime sector has implemented new programs and practices in an effort to enhance the security of our homeland. We look forward to continuing to work with TSA and Coast Guard on the TWIC program to ensure there are no unintended consequences and that the TWIC will be deployed in the most secure and efficient manner possible.

Thank you for the opportunity to speak today. I will be happy to answer any questions you may have.