TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

TESTIMONY OF

MAURINE FANGUY
PROGRAM DIRECTOR

TRANSPORTATION SECURITY ADMINISTRATION
THE DEPARTMENT OF HOMELAND SECURITY

BEFORE THE UNITED STATES SENATE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

October 4, 2007

Good morning Chairman Inouye, Vice-Chairman Stevens and distinguished members of the Committee. Thank you for this opportunity to share with you the significant progress we have made on the Transportation Worker Identification Credential (TWIC) program. I would like to acknowledge the leadership this committee has provided in defining the vision for TWIC.

The TWIC program is moving aggressively towards its objectives while making sound programmatic decisions focused on enhancing port security. I am happy to inform the Committee that enrollment will begin in Wilmington, Delaware later this month.

There have been a number of critical advances in the program since last spring:

- Completing test milestones on the enrollment system
- Adding TWIC enrollment sites based on stakeholder input
- Reducing the price of a TWIC card
- Establishing reader technical specifications
- Identifying card reader pilot participants and holding kick-off meetings

Completing Test Milestones on the Enrollment System

TWIC will impact the livelihoods of hundreds of thousands of American workers essential to the smooth flow of global commerce. Once TWIC is up and running, TSA will vet as many workers in one day as we did during the entire year-long prototype. The importance and enormity of this task within the maritime environment, with a dynamic and mobile workforce, has demanded a methodical approach with rigorous testing.

TWIC will be one of the world's most advanced, interoperable biometric credentialing programs and is powered by state-of-the-art technologies. We are nearly complete on our "flight test" of the full TWIC system, which has five main components:

- **Pre-Enrollment Web Site:** allows workers to schedule appointments and provide information ahead of time to make enrollment easier.
- **Enrollment Center:** captures a worker's biometric and biographic information and submits the information for security processing.
- **TWIC Core System:** routes applicant information for processing, conducts data integrity checks, and manages the status of TWIC cards.
- **Screening Gateway:** aggregates security threat assessment data from the FBI, Citizenship and Immigration Services, and watchlists. It is important to note that the Screening Gateway is used across all of TSA's vetting programs.
- **Card Production:** electronically loads an applicant's information onto a TWIC smart card and then physically produces the card.

All five of these parts were first tested individually. Next, these pieces were integrated to ensure the functionality of the end-to-end process of conducting accurate and timely security threat assessments and producing high quality credentials. In addition, security and privacy requirements were validated throughout the process. After our contractor verified system readiness, TSA completed independent verification before beginning final test enrollments in the field using live vetting on government and trusted contractor personnel.

Today we are in the final stages of field testing. The switch has been turned on and once field testing is completed, we will open the doors and begin enrollment in Wilmington, Delaware. After we verify successful enrollment operations in Wilmington, we will move forward aggressively to expand TWIC across the nation.

Adding TWIC Enrollment Sites

The TWIC final rule established a network of 130 enrollment sites located across the nation. Through collaboration with maritime stakeholders, we understand the importance of making enrollment as convenient and accessible as possible. We also have worked with the Department and our partners in the United States Coast Guard to reach out to stakeholders in the field and have identified additional locations for TWIC enrollment centers. At this time, we will field 146 fixed enrollment centers. In addition, we have worked with our contractor to add a mobile enrollment capability to take TWIC to the workers.

Reducing the Price of a TWIC Card

TWIC is a fee-based program paid for by applicants. We fully realize that these costs are significant and we are mindful of the need to identify areas for cost reduction. Recently, we announced that the fee for a standard TWIC will now be $132.50, a decrease from the price anticipated in the Final Rule. Workers with current, comparable threat assessments including HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade

(FAST)) will receive a discounted fee of $105.25. The cost of a lost, damaged or stolen credential is $60.

Establishing Reader Technical Specifications

The TWIC technical architecture is compatible with the credentialing standards established in Federal Information Processing Standard (FIPS) 201-1. This alignment is critical to support card and reader interoperability within the maritime mode. In response to comments received on the initial TWIC Notice of Proposed Rulemaking, TSA and the Coast Guard decided to remove the requirement for biometric readers from the TWIC final rule to allow time to establish technology specifications to support maritime operations.

TSA and the Coast Guard sought the advice of the National Maritime Security Advisory Committee (NMSAC) which established a working group to collaboratively develop new technical specifications that complement FIPS 201-1 and add features that will support high-volume physical access in the harsh maritime environment. The working group included representatives from both the maritime and technology industries.

TSA recently published the TWIC reader hardware and card application working technical specification. The working specification establishes the requirements for biometric card readers for the pilot projects required by the SAFE Port Act. These readers will be tested during the pilot program. As the card and readers are envisioned to operate when TWIC is fully implemented, use of a PIN will not be necessary to release the biometric, unless the owner/operator chooses to use contact readers and the contact side of the credential.

Identifying Card Reader Pilot Participants and Holding Kick-Off Meetings

As required by the SAFE Port Act, we have initiated pilot programs with five partners across the country to test card readers. The pilots will test access control technologies in real world marine environments. Our current list of participants includes the Port Authorities of Los Angeles, Long Beach, Brownsville, and New York/New Jersey, in addition to Watermark Cruises in Annapolis, Maryland. As part of the outreach efforts for the TWIC program and the Department's Port Security Grant Program, we continue to seek additional participants. Our objective is to include pilot test participants that are representative of a variety of facility vessels which operate in a variety of geographic locations and environmental conditions. There appears to be sufficient interest from the maritime community to achieve this objective.

We are in the process of finalizing the test approach for the pilots. We are working with DHS Science and Technology and the National Institute of Standards and Technology (NIST) to establish a test plan that will evaluate the card-reader interface under a variety of conditions and assess its impact on operations. Through the pilot tests, we will investigate the impacts of requiring biometric identity verification on business processes,

technology, and operational impacts on facilities and vessels of various size, type, and location. As the program proceeds, the pilots will inform the TWIC reader rulemaking process and ultimately result in final regulations that require the deployment of transportation security card readers consistent with the findings of the pilot program.

Lessons Learned and Future Efforts

We are proud of the significant progress we have made in the past six months and are mindful of the challenges ahead. As we move forward in the TWIC program, we are committed to incorporating our lessons learned to drive sound management decisions geared at improving all aspects of the program, including:

- *Look for efficiencies by eliminating duplicative regulatory processes.* TSA and Coast Guard are developing procedures for the sharing of fingerprints, identity verification, criminal history, and photographs for TWIC which is expected to save not only money but time. In addition, merchant mariners will no longer be required to visit a Regional Exam Center to obtain and renew their credentials, resulting in substantial time and travel savings.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meeting with operators and associations, and contributions of advisory councils all added great value. We came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting our ports.
- *Address the impact on small businesses.* TSA and the Coast Guard worked closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas. We are also producing and distributing a Small Business Compliance Guide to assist small businesses in their implementation of the program.
- *When practical, preserve State regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, the TWIC regulations do not preempt States from requiring background checks and badging systems for non-security purposes in addition to TWIC. States may need to set standards for important purposes other than terrorism threats, such as theft or organized crime.
- *Plan for privacy.* All data collected at an enrollment center will be completely deleted from the enrollment center work stations after transmission to TSA. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which is protected through role-based entry, encryption, and segmentation to

prevent unauthorized use. No paper records with personal identification information are created in the enrollment process.

- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emerging needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin performance-based contract award is a culmination of our efforts to date. We will continue to look for and implement adaptive program planning, contractor oversight, and metrics to ensure the success of the program.

- *Plan to address what issues may arise during testing.* Evolving technology, such as card readers, create a changing environment and program control constraints. This is especially the case when the technology must be deployed to a vast multitude of entities with remote connectivity challenges (e.g., vessels) and varying degrees of access control system capabilities.

Conclusion

The steps we are taking will be an extremely important aspect to the security of our port facilities and vessels. TSA will continue to work with our partners, the U.S. Coast Guard and maritime stakeholders, to ensure that for the first time in history thousands of independent businesses will have one, interoperable, security network and workers will hold a common credential that can be used across that entire network.

I appreciate the keen interest that this Committee has in an effective implementation of TWIC, and I thank you for your support. Mr. Chairman, this concludes my testimony and I am pleased to answer any questions that you may have.