UNITED STATES DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF MICHAEL JACKSON
DEPARTMENT OF HOMELAND SECURITY
DEPUTY SECRETARY

Before the

UNITED STATES SENATE
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

May 16, 2006

Good morning Chairman Stevens, Co-Chairman Inouye, and distinguished members of the Committee. Thank you for this opportunity to speak with you about the Transportation Worker Identification Credential (TWIC) program. The good news is that we are finally rolling this program out: two rulemakings and a procurement are now under way.

I am particularly grateful to this committee for its leadership in defining a vision and requirements for TWIC. In my previous position as Deputy Secretary of the Department of Transportation, I saw first hand the commitment of the members of this committee to TWIC. I think what DHS has done with our TWIC pilot test has produced real value-added by helping us create a program that will achieve our security goals, while also making good business sense. As we begin deployment, DHS will be building essential tools that we can use to streamline and coordinate credentialing and screening programs throughout the Department.

The two rulemakings that we have just initiated will align our current maritime security regulations with the framework of the TWIC program and credential. The procurement that we have announced seeks a single integrator to perform both the intake function of processing applicants for cards and also managing important parts of the data integration system. This system will connect each step in the credentialing process from intake, to background check, to card issuance. These rulemakings and procurement are the key steps to launching the TWIC program as a lynchpin of port security. We must know who has access to our ports and must have the ability to deny access to those who pose a security threat. Fundamental to our approach as we implement these steps to improve port security, is our commitment to do so without adversely affecting, either economically or logistically, our international trading system.

My testimony today will cover the following points:

- The Coast Guard's recent rule change on biographic background checks -- we are not waiting for the full TWIC roll-out but intend to get initial security benefits immediately;

- The rulemakings and their alignment with both the Maritime Transportation Security Act (MTSA) and the Merchant Mariner Credential; and
- The TWIC program framework, business model and implementation plans.

Background

Maritime security is an important part of our overall homeland security. TWIC will be a key component in a layered security system. It will complement our efforts both at home and abroad including cargo security tools, radiological and nuclear detection, the Customs-Trade Partnership Against Terrorism, the Container Security Initiative, and MTSA port facility programs. Security cannot be delivered via a single, silver bullet solution. This is particularly true with regard to the maritime sector. There, a layered system of security is needed to deal with the vast scale of the global system in which security responsibility is shared, where there is a multiplicity of private sector actors that have primary responsibility for implementing and performing most of the frontline security duties, and where the interests of numerous foreign governments must be addressed.

Domestically, an estimated 750,000 workers currently have unescorted access to our ports. To secure the 361 domestic port facilities, the Coast Guard, working with port operators, has approved the designation of certain "secure areas" within each maritime facility and vessel to which longshoremen, truckers and vessel crews would need a secure biometric identification credential in order to be granted unescorted access.

The TWIC deployment includes accelerated and parallel rulemakings by both TSA and Coast Guard. It also includes a much needed procurement to help launch the operational program. Secretary Chertoff has given his team instructions to get this done as quickly as possible. This tool will add another valuable layer of security to domestic port operations and will strengthen overall supply chain security.

Coast Guard Requires Interim Step of Biographic Background Checks

As a significant prelude to the final rollout of TWIC, the Coast Guard has exercised its legal authority to publish a notice requiring approved identification credentials for access to MTSA-regulated facilities. For certain credentials, this involves a preliminary biographic background check. The Coast Guard and TSA consulted with our industry partners to develop a process that compares a worker's biographical information against our terrorist watch lists and immigration databases. TSA has already begun to conduct these background checks, and any workers who pose a security risk will be denied access to these facilities.

The process is straightforward. Facility owners, facility operators and unions seeking a background check will submit an individual's name, date of birth, and, as appropriate, alien identification number to the Coast Guard. To speed up the review process, an

individual's social security number may be submitted, but is not required. This information will allow TSA to vet workers against terrorist watch lists through the Terrorist Screening Center. Moreover, these checks also include a review of a worker's immigration status, conducted by the U.S. Citizenship and Immigration Service using its Central Index System. As with other sectors of our economy, we will not tolerate the employment of illegal workers at our nation's ports or within any part of the maritime infrastructure.

This initial round of background checks, for which we have already begun to receive names, will cover an estimated 400,000 port workers and will focus first on employees and longshoremen who have daily access to the secure areas of port facilities.

Aligning Current Maritime Security Requirements with TWIC

Following enactment of MTSA in November 2002, the Coast Guard issued a series of general regulations for maritime security. Those regulations set out specific requirements for owners and operators of vessels, facilities, and Outer Continental Shelf facilities that had been identified by the Secretary as posing a high risk of being involved in a transportation security incident. Accordingly, owners and operators of these vessels and facilities were required to conduct security assessments, create security plans specific to their needs, and submit the plans for approval to the Coast Guard by December 31, 2003. All affected vessels and facilities are required to have been operating in accordance with their respective plans since July 1, 2004, and are required to resubmit plans every five years.

Each plan requires owners or operators to address specific vulnerabilities identified pursuant to their individual security assessments, including controlling access to their respective vessels and facilities. Most significantly, MTSA regulations require owners/operators to implement security measures to ensure that an identification system is established for checking the identification of vessel and facility personnel or other persons seeking access to the vessel or facility.

In establishing this initial identification system, owners/operators were directed to accept identification only if it: (1) was laminated or otherwise secure against tampering; (2) contained the individual's full name; (3) contained a photo that accurately depicted the individual's current facial appearance; and (4) bore the name of the issuing authority. The issuing authority had to be a government authority or organization authorized to act on behalf of a government authority, or the individual's employer, union or trade association. There was no requirement that the identification be issued pursuant to a security threat assessment because there was no existing credential and supporting structure that could fulfill the needs specific to the maritime environment at the time those regulations were created.

Now that the credential and supporting structure for TWIC has been developed, it must be integrated into this pre-existing security program though amendments to the current

regulations. While not prejudging the rulemaking process, I can state that we generally expect to adhere to the procedures that TSA has used to regulate the licensing of drivers who transport hazardous materials.

The Merchant Mariner Credential. Because MTSA in essence requires the TWIC for all U. S. merchant mariners, the Coast Guard took this opportunity to revise its merchant mariner credentialing system to streamline the process and remove any duplicative requirements that would exist as a result of the TWIC rulemaking. This was done through a separate rulemaking that will publish simultaneously with the TWIC rulemaking.

Under the current regulatory scheme, the Coast Guard may issue a mariner any combination of 4 credentials: (1) Merchant Mariner Document (MMD); (2) License; (3) Certificate of Registry (COR); or (4) Standards of Training, Certification, and Watchkeeping (STCW) Endorsement. The License, COR and STCW Endorsements are qualification credentials only. Only the MMD is an identity document, and none of the current mariner credentials contain the biometric information required under MTSA. Because of this, the Coast Guard has drafted a proposed rule that would combine the elements of these 4 credentials into one certificate called the Merchant Mariner Credential (MMC). The MMC would serve as the mariner's qualification credential, while the TWIC would serve as the mariner's identification credential. Mariners would have to have a TWIC before they could be issued an MMC.

To further ease the burden on mariners who now must appear at one of 17 Coast Guard Regional Examination Centers (RECs) at least once in the application process, the Coast Guard and TSA have come to an agreement to share information submitted in the TWIC application process. As proposed in this MMC rulemaking, TSA would provide the Coast Guard with electronic copies of the applicant's fingerprints, proof of identification, proof of citizenship, photograph, and if applicable the individual's criminal record, FBI number and alien registration number. This information would then be used in reviewing the applicant's safety and suitability for the credential and the Coast Guard would not conduct an additional security threat assessment. Applicants would no longer be required to visit an REC unless they had to take an examination. This proposed change is expected to result in cost savings to the public as much of the inland population currently must travel great distances to reach an REC.

The consolidation of qualifications credentials and a further streamlining of other mariner regulations is a positive and meaningful development that will ensure that no mariner is required to undergo more than one security threat assessment or criminal background history check.

The TWIC Program

National security interests require that individuals seeking unescorted access to MTSA-regulated vessels and facilities be properly identified and undergo appropriate

security vetting. Furthermore, facilities and vessels need a reliable tool for identifying those individuals who have been granted such access. For that reason, TSA has been developing the TWIC, which is a 21st century identification card for transportation workers. The TWIC card will include biometric technology that is intended to make it virtually impossible for the card to be used by anyone other than the person to whom the card was issued. Although implemented only in the maritime sector now, in time TWIC is expected to streamline the background check procedure across our Nation's transportation system.

The TWIC maritime program has been designed to satisfy the following mission goals:

- Identify authorized individuals who require unescorted access to secure areas of MTSA-regulated facilities and vessels;
- Determine the eligibility of an individual for access through a security threat assessment;
- Ensure unauthorized individuals are denied access through biometric confirmation of the credential holder;
- Revoke immediately access for individuals who fail to maintain their eligibility;
- Apply privacy and security controls to protect TWIC information; and,
- Fund the program entirely by user-fees.

To achieve these goals, TSA and the Coast Guard promulgated a joint TWIC notice of proposed rulemaking (NPRM) for the maritime sector. Under Secretary Chertoff's direction, the joint rulemaking process between the Coast Guard and TSA has been accelerated. Both the NPRM as well as the Coast Guard's rule on the Merchant Mariner Card were sent to the *Federal Register* on May 10 and it has been posted on TSA's web page. Under the joint rule, the DHS, through the Coast Guard and TSA, formally proposes to require that all U. S. merchant mariners and all persons who need unescorted access to secure areas of a regulated facility or vessel must obtain a TWIC.

In order to obtain a TWIC, individuals will be required to undergo a security threat assessment conducted by TSA. TSA, in conducting those security threat assessments, will use the procedures and standards similar to those that apply to commercial motor vehicle drivers licensed to transport hazardous materials within the United States. It is anticipated that program implementation will begin at the end of 2006.

TSA has already tested the technology and the business process required to implement the TWIC. During the testing phase, which ended in June of 2005, more than 4,000 of these credentials were issued to transportation workers at 26 locations in six states. We have proven that this technology can work in the field.

Scope. We expect these cards will eventually be issued to about 750,000 workers who have unescorted access to secure areas of MTSA-regulated maritime port facilities and vessels. TWIC cards will be required not only for port facility workers, but for anyone who seeks unescorted access to secure areas of a MTSA regulated facility or vessel, regardless of frequency, such as certain crew members, truck drivers, security guards, and

rail employees, as well as all U. S. merchant mariners who hold an active U. S. Merchant Mariner's License (License), Merchant Mariner's Document (MMD), Certificate of Registry (COR) or STCW Endorsement. Future rules would be required to incorporate additional sectors (modes) of the transportation population such as air and rail.

Security Threat Assessment. The security threat assessment for TWIC will include a review of criminal, immigration, and pertinent intelligence records to determine whether the individual poses a threat to transportation security. As previously noted, the TWIC process will mirror that of the Hazardous Materials Endorsement (HME) regulations and will integrate with them. TSA first issued regulations to implement security threat assessment standards for HME applicants -- TSA's hazmat rules -- in May 2003 and subsequently amended those regulations based on comments received from the States, employers and affected drivers.

TSA's hazmat rules establish standards concerning criminal history, terrorist activity, mental capacity, and immigration status to determine whether a driver poses a security threat and is qualified to hold an HME. Drivers who have been convicted or found not guilty by reason of insanity for certain crimes in the preceding 7 years, or have been released from incarceration for those crimes in the preceding 5 years, are deemed to pose a security threat and are not authorized to hold an HME. Drivers convicted of certain particularly heinous crimes, such as espionage, treason, terrorist-related offenses or severe transportation security incidents, are permanently banned from holding an HME. In addition, drivers who have been involuntarily committed to a mental institution or adjudicated as mentally incapacitated are considered to pose a security threat that warrants disqualification from holding an HME.

Aliens are not prohibited from obtaining an HME. The hazmat rule permits individuals who are in the United States lawfully and are authorized under applicable immigration laws to work in the United States to hold an HME upon completion of a satisfactory TSA security threat assessment. As set forth in the hazmat rules, an applicant's immigration status is reviewed and TSA conducts a security check of international databases through Interpol or other appropriate means.

Right of Appeal. TSA will establish a comprehensive TWIC redress process under which individuals will have the opportunity to appeal an adverse determination or apply for a waiver of the standards. TSA's current hazmat rules include appeal and waiver procedures to ensure that no driver is wrongfully determined to pose a threat, and to provide individuals who are disqualified from holding an HME the opportunity to show rehabilitation, where applicable. Similar procedures are proposed for TWIC.

Technical Standard. The TWIC technical architecture does not conflict with HSPD-12 and FIPS-201 requirements and will provide an open standard that will ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector.

Funding. Initial costs of implementing TWIC will be borne by the Department's budget as we bring the outside integrator on board and transition current DHS system to the contractor. After that initial, transition stage, all costs of the program will be borne by TWIC applicants. TSA will take into account the fees paid by HME holders and merchant mariner applicants to ensure that duplicate threat assessments are not performed and duplicate fees are not collected. Nevertheless, there will be some additional fees associated with the cost of actually issuing and activating a TWIC to this subset of applicants that they will have to bear.

Rulemaking Outreach. We know it is of vital importance to reach out to stakeholders and use their input to shape this program and rulemaking. Informal discussions have taken place already as we completed the TWIC pilot phase. Going forward, TSA and the Coast Guard will hold public meetings over the next few months in Newark, NJ, Tampa, FL, St. Louis, MO and Long Beach, CA. Interested individuals will be invited to attend, provide comments and ask questions about the proposed rule. TSA and Coast Guard will provide exact locations and other additional information about the meetings in another Notice to be published in the *Federal Register*.

Integrator Procurement. The Department will conduct a full and open competition for one integrated solution for the TWIC implementation. TSA intends to issue a new solicitation for TWIC enrollment services and the operations of the integrated data management system, including system maintenance. This will streamline the contracting and implementation process by identifying one party to fit all the pieces together into an effective, integrated security process. TSA has assessed alternative business models for TWIC implementation, and based on a full review of the total system time, risk, and cost of other options, has decided to go forward with a single integrator model.

Timing. Under the current timeframe, it is anticipated that DHS will begin to issue TWIC cards to workers at the first group of ports before the end of this year. We will work with the enrollment vendor and our port industry partners to select appropriate enrollment locations to serve all U. S. ports. We will rate each location against a variety of factors to assess criticality, population, and infrastructure to determine the best priority for enrollment, taking into account the cost and potential efficiency of conducting enrollments in several ports in the same region of the country at the same time.

The steps we are taking will be yet another boost to the security of our port facilities and vessels. It's an effort which, when completed, will assure our citizens that those people who have unescorted access to secure areas of these port facilities and vessels have been screened to make sure that they are not a security threat.

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'm pleased to answer any questions that you may have.