TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC)

TESTIMONY OF

KIP HAWLEY
ASSISTANT SECRETARY

TRANSPORTATION SECURITY ADMINISTRATION
THE DEPARTMENT OF HOMELAND SECURITY

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

April 12, 2007

Good morning Chairman Inouye, Vice Chairman Stevens, and distinguished members of the Committee. Thank you for this opportunity to speak with you about the Transportation Worker Identification Credential (TWIC) program.

I would like to acknowledge the leadership this committee has provided in defining the vision and requirements for TWIC. The TWIC program is moving aggressively towards its objectives with a focus on making good security and business decisions. This leading edge program is developing essential processes, capabilities and expertise that will be beneficial to other programs.

The final rule for TWIC went into effect on March 26, 2007. With the passing of this critical milestone, this hearing provides an excellent opportunity to highlight program developments and describe how we are incorporating our lessons learned into an effective, efficient business plan for TWIC enrollment.

We have framed our program decisions and processes within the context of the nation's port security goals, including the need to:

- Identify authorized individuals who require unescorted access to secure areas of Maritime Transportation Security Act (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 access promptly 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.

Achieving these ambitious goals has required creative planning, flexible implementation, effective stakeholder communication, and adaptive contract management. The basic

program deployment philosophy has been a commitment to evaluate all practicable technical alternatives that will provide adequate port security and minimize adverse impacts, either economically or logistically, to our nation's citizens and our international trading system. This has been and will continue to be the program's implementation premise.

TWIC Milestones to Date

An estimated 750,000 workers currently have unescorted access to our ports. The central technical TWIC challenge is providing facilities and vessels with a reliable tool for identifying individuals who have been granted authorized access to our ports. Simply put, TSA has been tasked with the development of a 21st century identification system. The key element of the system is a card that includes biometric technology that makes it virtually impossible for the card to be used by anyone other than the person to whom the card was issued.

The technical principle underlying TWIC's ability to authenticate a person's identity includes three factors. When using the full extent of TWIC's authentication ability each person can be identified by:

- Something they know – a worker's Personal Identification Number (PIN);
- Something they have – the TWIC credential; and
- Something they are – a biometric.

Obviously, new processes and technologies require systematic pilot studies. The prototype study was deployed to 26 locations in the areas of Los Angeles/Long Beach, Wilmington/Philadelphia and Florida's deepwater ports. The prototype TWIC was successfully issued to more than 4,000 volunteer workers including truck drivers, longshoremen, container terminal, railway, and airport personnel. A name-based threat assessment was completed on each individual. A criminal background check was conducted by the State of Florida for the deep-water port volunteers. These efforts were a success on multiple levels; it provided invaluable experience and a much deeper understanding of the technical and logistical challenges.

Security improvements could not wait until TWIC is fully deployed. We have gone forward with significant interim security enhancements and actions during TWIC's initial development phase. These actions included:

- The Coast Guard worked effectively with National Maritime Security Advisory Committee (NMSAC) to define secure areas. This definition will have a direct impact on over 10,000 vessels and more than 3,200 facilities. These secure areas delineate where a TWIC will be required for unescorted access.
- The joint rulemaking process between the Coast Guard and TSA was accelerated resulting in TWIC Notice of Proposed Rulemaking (NPRM) being published on May 22, 2006.

- The Coast Guard and TSA worked with industry partners to develop an interim process that compares a worker's biographical information against our terrorist watch lists and immigration databases.
- Facility owners, facility operators and unions submitted worker names, date of birth, and, as appropriate, alien identification number. The worker's immigration status was checked by the U.S. Citizenship and Immigration Service using its Central Index.
- To date TSA has completed 740,000 name based threat assessments on port workers and longshoreman. These assessments were an interim measure and did not include the criminal history records check or biometric credential that is part of TWIC.

TWIC Rule and Stakeholder Input

The TWIC rule was posted on the TSA and Coast Guard websites on January 1, 2007, and published in the Federal Register on January 25, 2007. The rule is the result of extensive public involvement and interagency coordination. In addition to the direct involvement of the National Maritime Security Advisory Committee, TSA and the Coast Guard held four public meetings in Newark, NJ, Tampa, FL, St. Louis, MO and Long Beach, CA. Over 1,900 comments were received from workers, port owners and operators, small businesses and others affected by the new program. All comments were carefully considered and we made significant changes to the NPRM in the development of the Final Rule. These changes include:

- The Coast Guard and TSA delayed the requirement to purchase and install electronic readers to allow for additional field testing, technology improvements, and more public comment.
- We created an expedited interim threat assessment process for new hires so that they may go to work pending completion of the full threat assessment.
- We expanded the immigration requirements to permit certain Visa-holders who are prevalent in the maritime industry to apply for TWIC.

In addition, the TWIC NPRM and Final Rule include provisions that respond to comments we received from workers subject to similar threat assessment programs. These include:

- Creating a new process where TSA can make a determination that a security threat assessment conducted by another government agency is comparable, eliminating redundancy and reducing costs for workers;
- Providing workers more time to apply for an appeal or waiver;
- Streamlining the process, jointly with the Coast Guard, for merchant mariner credentialing and ensuring that there was no duplication of requirements resulting from the TWIC process.

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. The workers covered by this rule include certain truck drivers, rail employees, security guards, longshoremen, as well as all U.S. merchant mariners. TSA will use the time tested security assessment procedures and standards that are currently used for commercial motor vehicle drivers licensed to transport hazardous materials, known as Hazardous Material Endorsements (HME). In short, TWIC will be issued to workers who successfully complete a security threat assessment, which includes: (1) a check against terrorist watch lists, (2) an immigration status check, and (3) a FBI fingerprint-based criminal history records check.

TWIC Card Readers

The TWIC rule does not currently include a requirement for owners and operators to use card readers. This was done as a response to important public comments received on the NPRM and concerns from Congress expressed in the SAFE Port Act. The card reader requirement is being formulated and coordinated by extensive technical input from industry and the public. In the interim, workers seeking unescorted access to secure areas will present their cards to authorized personnel, who will compare the photo, inspect security features on the card, and evaluate the card for signs of tampering. At facilities with various sophisticated access control systems, the magnetic stripe on the credential could be used to grant or deny access at entry gates. The Coast Guard will also institute periodic unannounced checks to confirm the identity of the holder of the TWIC.

We will continue to work closely with all interested parties to address the ever evolving technology issues. The TWIC technical architecture is compatible with Homeland Security Presidential Directive (HSPD) 12 and Federal Information Processing Standards (FIPS) 201-1 requirements which provide an open standard that will ensure interoperability and real-time exchange for supply chain security cooperation between the Department and the private sector. The applicant's photograph, name, TWIC expiration date, and a unique credential number are printed on the card. An integrated circuit chip on the card stores two fingerprint minutia templates and a PIN as well as a digital photo of the applicant, the applicant's name, and card expiration. The embedded computer chip is capable of being read by both contact and contactless card readers and also contains the magnetic strip and linear bar codes.

In addition to previously conducted prototype testing, pilot test planning and discussions with interested port, facility, and vessel operators began late last year. The pilots will test access control technologies in real world marine environments. The National Maritime Security Advisory Committee is providing invaluable input regarding operational requirements and has recommended specifications for contactless biometric smart cards and card readers. Public feedback is being collected and analyzed on the recommendations. As part of the outreach efforts for the TWIC program and the Department's Port Security Grant Program we have met with a number of maritime interests to invite their participation in the pilot tests. Our objective is to include pilot test participants that are representative of a variety of facility and vessel types and sizes

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.

The Department is currently reviewing Port Security Grant applications relating to these pilot studies and will announce awards later this spring. While the grant process is proceeding, TSA and Coast Guard are working with Department test and evaluation experts to develop a comprehensive plan that addresses the unique pilot test challenges. The evaluation of the pilot tests will greatly facilitate the Department's efforts to propose a TWIC reader requirement rule that effectively addresses security requirements, maintains the flow of commerce, and protects the personal information used to validate the TWIC holder's identity.

Rollout Contract

A key operational piece of the rollout plan was the award of a competitively bid, indefinite delivery/indefinite quantity contract to Lockheed Martin Corporation. The TWIC enrollment and systems operations and maintenance contract will include a Quality Assurance Surveillance Plan (QASP) that establishes detailed metrics to be monitored through the life of the contract and will determine whether the contractor will receive any award fee for services performed.

Lockheed Martin will establish approximately 130 enrollment centers near the port facilities where applicants will provide biographic information and fingerprints. This information will be transferred to TSA so we may conduct a threat assessment involving checks of criminal history, immigration, and intelligence databases. Once a worker successfully completes the threat assessment process, the government will produce the credential and send it to the enrollment center, where the worker will retrieve it. TWIC enrollment will begin initially at select ports based on risk and other factors and will proceed throughout the nation over the next 18 - 24 months.

TWIC Card Costs

As required by Congress, the costs of the program will be borne by TWIC applicants. Therefore, we are obligated to look for practicable ways of controlling costs, eliminating duplicative processes, providing timely decisions, and, most importantly, ensuring accuracy and fairness.

The fees for a TWIC will be slightly lower than was anticipated in the Final Rule. A TWIC will be $137.25 for a card that is valid for 5 years. Workers with current, comparable background checks (e.g., 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 $36, although we have solicited comment on raising that fee.

We fully realize that these costs are not an insignificant amount to some workers. However, we feel that the costs compare very favorably with equivalent HSPD-12 compliant card fees and in some instances may actually reduce the costs for some workers. For example, the Coast Guard is in the process of completing a companion rule which will consolidate existing mariner credentials and streamline the application process for mariners who have already applied for the TWIC. This will reduce the overall cost burden for these workers. Preparations are underway to reduce duplication by having TSA 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 will eliminate the need for TWIC holding mariners to visit a Coast Guard Regional Exam Center to apply for or renew their Merchant Mariner Credential unless an examination is required.

Rollout Communication Plan and Pre-Enrollment

Effective public communication is fundamental to our rollout plan. The TWIC program office has used the lessons learned from the prototype phase to develop a multi-dimensioned outreach strategy for all of the enrollment phases. A toll-free help desk, Frequently Asked Questions, informational brochures, and a centralized e-mail address will provide up-front assistance and guidance for workers, owners, and operators. These services include program information, response to enrollment questions, pre-enrollment assistance, lost/stolen card reporting, credential replacement support, updates on an individual's case, and information on appeals and waivers. Applicants are encouraged, but not required, to "pre-enroll" and provide biographic information at the secure TWIC web site which should help reduce waiting time at the enrollment centers. An additional service that is provided during pre-enrollment is an opportunity for the applicant to schedule an appointment for appearing at the enrollment center.

Lockheed Martin is required by contract to develop a communication plan to ensure that applicants, operators, and relevant industry associations are educated and knowledgeable about the TWIC enrollment process. The communication plan will identify TSA goals and responsibilities, contractor goals and responsibilities, port facility and vessel responsibilities, target audiences, communications processes, and supporting communication tools. A key plan element is the use of a communication committee to ensure sustained two-way communication with major stakeholders. This vital effort is calculated to provide the most current, accurate program information to interested stakeholders and provide a mechanism for continuing stakeholder input during the rollout.

Enrollment Centers

Enrollment sites will be operated by trusted agents who are employees of a vendor under contract with TSA. These trained agents will have undergone a TSA security threat assessment before being allowed to collect the data. The trusted agents will provide applicants with a privacy notice and consent form, by which the applicant agrees to provide personal information for the security threat assessment and credential. The

trusted agents will verify an applicant's identity, confirm the accuracy of biographic information, collect biometric information (a full set of fingerprints and a facial photograph), and obtain the applicant's signature on the enrollment documents. The contract performance parameter for the trusted advisor enrollment process will be an average enrollment time of 15 minutes. The enrollment process for a pre-enrolled applicant is fully expected to take less time. As you can see, focused planning that fosters convenience for applicants will benefit workers as well as our process efficiencies.

Data Security Vetting and Card Issuance

After enrollment, an applicant's data is sent to the TSA system, and the vetting process (i.e., terrorism database, criminal history records check, immigration check) is started. We anticipate that the TWIC threat assessment processing time will be similar to our experience in the HME program. Since the inception of the HME program, threat assessments have frequently been completed in 3 days or less. During this same period the average time for completing HME threat assessments has been approximately 14 days, which includes all appeals and waivers. The process will be impacted by steps where there is minimum governmental control. For example, applicants need to promptly provide corrected records, and respond to initial determinations. Other factors that we anticipate could result in processing delays include an applicant providing incorrect information, watch list determinations, evaluation of the nature of threats, whether the applicant is currently under criminal investigation, and confirming immigration status that is not available in electronic format. Nonetheless, the 14 day average for processing the HME assessments includes the time required to meet the same threat assessment challenges that we will face with TWIC.

If TSA determines that an applicant does not pose a security threat, the applicant's information is sent for card production. After the card is developed it is sent to the enrollment center, where the worker will be notified to pick up the card. Due to the secure nature of the credential, the smart cards are shipped as "inactive." An applicant must verify his or her personal identity by providing a biometric (i.e., fingerprint) that is matched to the cards electronic template. After identity is verified, the applicant selects a secret PIN which is stored on the card as an additional identity authentication factor.

Worker Redress/Waivers/Appeals

If an applicant is denied a TWIC they will be notified of the reason and instructed on how to apply for an appeal or waiver. All applicants have the opportunity to appeal a disqualification and may apply to TSA for a waiver. In order to expedite processing time, applicants who are aware of a potential disqualifying crime may begin the waiver process when they initially apply for a TWIC.

The standards for denial of a TWIC are the same standards that apply in the HME process. Any applicant who is subject to removal proceedings or an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC. An

individual will be disqualified if he or she lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

A person will also be denied a TWIC for a criminal history involving certain disqualifying crimes. TSA received valuable NPRM comments on the list of disqualifying crimes and decided to fine tune the list to better reflect crimes that are more likely to result in a terrorism security risk or a risk that the individual may engage in a transportation security incident. Permanent disqualifying criminal offenses include: espionage, sedition, treason, terrorism, improper transportation of a hazardous material, unlawful possession, use or sale of an explosive, murder, threats to a place of public use (government facility, public transportation system, or infrastructure facility), violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act in which the predicate act is one of the permanently disqualifying crimes, or a crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Individuals are ineligible for a TWIC if convicted in the last seven years or incarcerated within the last five years of the following crimes: Unlawful possession, use or sale of a firearm or other weapon, extortion, fraud, bribery, smuggling, immigration violations, distribution or importation of a controlled substance, arson, kidnapping or hostage taking, rape or aggravated sexual abuse, assault with intent to kill, robbery, RICO violations that do not involve a permanent disqualifying crime.

The appeal process involves ensuring that the information on which TSA bases its threat assessment is completely accurate. This process allows the applicant to correct the record on which that threat assessment occurs.

Fairness and accuracy in TWIC waiver determinations are further ensured by an opportunity for independent review by an Administrative Law Judge. As previously noted, the regulations provide a lengthened period for appealing denial of waivers, from 30 days to 60 days, to accommodate workers who tend to travel for extended periods of time. Furthermore, the regulations allow a worker to file a request for a time extension after the deadline has passed by filing a motion describing the reasons why they were unable to comply with the timeline. The extra procedural measures are intended to give workers every reasonable chance to bring legitimate concerns and issues to the attention of people who are trying to make the best and correct decision regarding security risks.

Lessons Learned and Future Efforts

The initial rollout of TWIC will be focused on the maritime mode. However, once the initial maritime rollout is complete DHS will evaluate deployment of this program in other modes of transportation. The analysis and planning for any resulting decision will benefit from the experience, technical expertise, and lessons learned that evolved under the TWIC program.

There are several vital lessons learned during the development of this program that must be prominently considered in future efforts:

- *Look for efficiencies in duplicative regulatory processes.* As noted previously, TSA and Coast Guard are developing procedures for the sharing of mariner 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.
- *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 practicable, preserve State regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, TSA does not preempt States from requiring background checks and badging systems in addition to TWIC. States may need to set standards for important purposes other than terrorism threats, such as preventing drug trafficking or organized crime.
- *Plan for privacy.* All data collected at an enrollment center will be deleted from the enrollment center work stations. 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.
- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emergent needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin contract award is a culmination of our efforts to date. Due to the nature of this task, however, we will need to continue to look for and implement adaptive planning, metrics, and changes to ensure this effort stays on track.
- *Don't expect a "silver bullet" technology solution.* Evolving technology, such as card readers, creates 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.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meetings with operators and associations, and contributions of advisory councils all added pure 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.

Conclusion

The steps we are taking will be an extremely important aspect 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 am pleased to answer any questions that you may have.