S. HRG. 109–1112

TRANSPORTATION SECURITY ADMINISTRATION'S TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROGRAM

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MAY 16, 2006

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

64–227 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
KENNETH R. NAHIGIAN, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

WITNESSES

APPENDIX

TRANSPORTATION SECURITY ADMINISTRATION'S TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROGRAM

TUESDAY, MAY 16, 2006

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:40 a.m. in room SD–562, Dirksen Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Well, we apologize. It's hard to set the time for commencing a hearing now, with the process we're going through on the immigration bill. We do thank you very much. We want to welcome the witnesses who will appear before the Committee, and thank them for their willingness to participate in this hearing.

The purpose of our hearing is to examine the status of TSA's Transportation Worker Identification Credential, commonly known as the TWIC program. The emphasis of our discussion will be to review policy and management issues that have prevented TSA from fully launching this program.

The Commerce Committee first authorized the Transportation Worker Credential in the Aviation Transportation Security Act of 2001, then again in 2002 and 2004, when the Committee developed and reauthorized the Maritime Transportation Security Act. These laws authorized the development and issuance of biometric security cards to transportation workers who satisfied background checks for entry to secure areas in the maritime as well as secure transportation facilities.

In authorizing the TWIC program in each of these measures, this committee recognized that our ability to secure the Nation's ports hinges upon our ability to verify, in a timely manner, the identity of port workers and prevent unauthorized access to secure maritime areas when necessary. The current inability of port operators to identify who's on their property at any given time should be considered a significant security vulnerability that must be addressed immediately.

Evidence of the need to verify the identities of workers at our ports occurred in my home state in 2003 during the 2-day lockdown of the Alyeska Pipeline terminal at the Port of Valdez during a

heightened terrorism alert. Terminal officials spent hours sifting through the employee documentation databases in an effort to determine who was on the port premises. Had the TWIC program been in place, officials would have been able to quickly determine which employees were authorized to be in secure areas of the terminal, which would have allowed officials to focus on the threat situation.

Despite a stipulation among stakeholders that interoperable TWIC programs would significantly enhance security at the Nation's ports, the program has experienced internal and external challenges. While TSA has struggled with timely decisionmaking, vendors, port authorities, states, and other stakeholders have complained about the lack of communication. Secretary Chertoff announced, on April 25, that DHS would begin conducting name-based background checks on the initial group of 400,000 maritime workers throughout the U.S. This is an encouraging step toward full realization of the program, but it has been over three and a half years since Congress first authorized the Transportation Workers Credential. Therefore, Senator Inouye and I have introduced, along with 40 other cosponsors, a bill that would set a hard deadline for TSA to launch the program. We believe the program is too vital to port security to risk more delays.

We look forward to seeking answers in questions today. We thank you very much for coming. I want to state that I have examined both the Los Angeles Port and the Seattle Port, and had a full briefing in Seattle of their security measures. They're very costly security measures, I might add. And so, we can understand some of the delay.

Senator Inouye?

STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. Well, I thank you very much. As you've indicated, Mr. Chairman, this program has been plagued by cost overruns and missed deadlines, and has produced few positive results.

A background check program, for example, of truck drivers driving hazardous materials has been criticized for its poor conception and high cost. The program for the maritime sector, by most accounts, is still at least 2 years away. And I join the Chairman in offering our assistance in bringing this matter to some resolution. There are many people who are nervous about this, and I commend you for what you're doing, but I think you need some of our help.

Thank you very much. May I have the whole statement made part of the record?

The CHAIRMAN. Without objection, yes, sir.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Following the attacks on September 11, 2001, the Congress recognized that it not only had to improve the security of the Nation's transportation infrastructure, it had to improve the security of its transportation workforce as well.

The Transportation Workers Identification Credential (TWIC) program was specifically created to provide thorough and efficient background checks of all transportation workers, yet 5 years later, the program has made very little progress.

As required by the Aviation and Transportation Security Act (ATSA), the Administration was able to conduct hundreds of thousands of background checks on airline employees in a relatively short time period. This speedy effort to evaluate aviation workers helped restore the traveling public's confidence in commercial air service and helped minimize the economic damage. As a result, air travel continues to expand and is now in greater demand than at any previous point in aviation history.

Because of the Congress's direction and the tragedy's impact on the economy, the Administration acted with an extreme sense of urgency in the immediate, post-September 11 environment when it came to aviation. That sense of urgency has all but disappeared for other modes, and the Administration's work on TWIC proves it.

The program has been plagued by cost overruns and missed deadlines and has produced few positive results. The background check program for truck drivers driving hazardous materials has been criticized for its poor conception, redundancies, and high costs. The program for the maritime sector, by most accounts, is still at least 2 years away from being deployed.

There have been no successful attacks on our transportation systems since September 11, and while that is obviously laudable, it is no guarantee of future success. The TWIC program is an important component of our transportation security system, and it must move forward. It has remarkable potential to eliminate key vulnerabilities and improve operational efficiency.

This potential can only be achieved if the requisite sense of urgency is restored. If the Transportation Security Administration (TSA) cannot motivate itself to turn TWIC around, then it will be up to Congress, through far more vigilant oversight, to provide the motivation. Too much time and money have been wasted already.

The CHAIRMAN. And your statement will appear in the record in full, Mr. Jackson. We thank you very much.

We're going to hear first from Michael P. Jackson, the Deputy Secretary of the Department of Homeland Security.

Thank you, sir.

STATEMENT OF HON. MICHAEL P. JACKSON, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Mr. JACKSON. Mr. Chairman, thank you very much for having me here today. And, Senator Inouye, thank you for your support, as well as that of the Chairman, for this important program.

I know of the work of this Committee from my time as Deputy Secretary of Transportation, and I know of the founding-father role that was played in this Committee to help make TWIC an important priority for this Nation. I will tell you that Secretary Chertoff, myself, the TSA share this commitment. The Coast Guard has to participate; it shares this commitment. CBP is in a supporting role; and they share this commitment.

We did a review, when Secretary Chertoff came onboard, of things that needed doing that were taking too long. This was definitely on the list of those topics. We have done a thorough scrub of the pilot phase of this. I will say that it was harder than perhaps was anticipated at first, and more complex. We have integrated the work that's being done here to other Federal programs and other standard-setting activities so that we have a solid base technologically and operationally by consulting with our stakeholders in this. But I will tell you today that this has the highest priority commitment of the Department for a deployment that we will say will begin this year in issuance of TWIC cards for maritime workers.

So, Mr. Chairman, I'll just be very brief in providing a top-line overview, and then be happy to answer questions about how we'll make good on that commitment.

What I would tell you is just a brief word about the context for this. The legislation that you're working on in the maritime world, and our discussions of maritime security, have this placed into a context. We're worried about—four things that we're worried about: ships, workers, cargo, and facilities. And we're worried about having to find good tools to use—or we're focused on finding good tools to use in those four categories at home and abroad. So, ships, cargo, people, facilities.

This discussion of bringing greater clarity to who is having unescorted access to our port facilities is an absolutely crucial component of that overall mix of the layered system of systems that we need to bring to the maritime domain. I would just say that the way to get this out on the street and operating begins with a rulemaking process and a procurement process. It is leveraging the significant work that we've done as a pilot with three state areas and multiple facilities within those areas. We will start with a procurement that's—I mean, a piece of regulatory work that's on the table right now at the *Federal Register*. This lays the framework for how we integrate the Coast Guard programs, and they're responsible, under the maritime security regime, MTSA, and how this TWIC process fits into it. That's a NPRM that will have a relatively quick turnaround. We hope that will allow us, this summer, to get a final rule out on the street and have the architectural framework of how we will implement this, clear and certain, for all of our constituents in the private sector.

Second, we will undertake a procurement which we have launched. Today we will put out a solicitation for qualified candidates to allow us to narrow the field of candidates that will be capable of helping us manage some of the core work of the TWIC deployment.

So, the combination of rules and the procurement to get the private-sector partner necessary to help us integrate this will give us the core elements of moving forward.

What that procurement does is allow us to have a single integrator that will help work issues, from the capture of biometric identifiers and the data that's needed for enrollment through the process of managing the vetting and integration of the data management to check for the various areas of security clearance, which are criminal history record checks, terrorist watch-list checks, legal immigration status, outstanding wants and warrants.

So, we will have that integration. We will pass off the decisions to TSA to approve or disapprove any questionable cases, and we will then manage a card production and distribution cycle.

So, these are the core moving parts of what we need as tools to get this done, and we're committed to moving these at the very fastest pace consistent with discipline, economic and effective procurement, and regulatory work.

So, perhaps, sir, that—I would just stop with that brief overview of the moving parts. My written testimony describes this in more detail. And I'd be grateful, honestly, to help you unpack this in any way that would be useful.

I would just say, in conclusion, that we do very much appreciate the focus that this Committee brings to pressing on the urgency of

TWIC. I will tell you the leadership team, again, shares that very much.

[The prepared statement of Mr. Jackson follows:]

PREPARED STATEMENT OF HON. MICHAEL P. JACKSON, DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

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 firsthand 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 watchlists 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 5 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 facili-

ties 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 time-frame, 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.

The CHAIRMAN. That's very fair. Thank you very much for making it short.

We have, already, a system in place for the Hazmat clearances through FBI, which the truckers pay for. Now, will this be a redundant fee they have to pay to get the TWIC screening process?

Mr. JACKSON. No. In fact, if you have a Hazmat certificate that has already allowed us to do the background investigation components, then you would be able to achieve a TWIC at a reduced rate.

The CHAIRMAN. So, if the hazardous material handlers have that Hazmat certificate by the FBI, they will be all right.

Mr. JACKSON. They would still have to get a card, so they would pay a fee for the card and would go through the enrollment process, but the card would be less expensive to them, because we would not need to replicate those portions of the background work that have already been done in order to give them the Hazmat license. So, we're handing out a new identifier, which wasn't done with the Hazmat review.

The CHAIRMAN. Are there any restrictions for the TWIC that will not be required for Hazmat?

Mr. JACKSON. On the criminal history background check, we have aligned in our NPRM the requirements for the hazardous material and the TWIC for maritime world. So, the same type of offenses that would exclude you from getting a hazardous materials certification would exclude you from the TWIC card. That is a subject of our Notice of Proposed Rulemaking, so we're soliciting comments from the industry about whether, and to what extent, those two should remain in perfect alignment. But we have gathered that data on the TWIC—I mean, on the hazardous material——

The CHAIRMAN. Will the cards be valid for the same period of time?

Mr. JACKSON. Under the—the TWIC card is substituting for the hazardous material, with a new biometric card. And so, it's not a substitute for the hazardous material; it's a—that is, in essence, a—an addition to your commercial driver's license certification.

The CHAIRMAN. So, the Hazmat endorsement does not require biometric clearance?

Mr. JACKSON. It does. But—fingerprints, yes, sir. So, for example, that would be another example of: if we've taken your fingerprints for Hazmat, we don't need to take them again for TWIC.

The CHAIRMAN. We're going to a series of clearances that your Department is going to handle—Secured Flight, Registered Travel, TWIC—and you'll be running into things like Hazmat and other entities. Is there any chance to get them all together so that a person who's going to be in three different zones will be able to have just one card?

Mr. JACKSON. Yes, sir, and that's an excellent question. We are trying to find an architecture and, where possible, cards that will give us multiple uses. For example, we have the TWIC program, but we also have border-crossing cards: NEXUS, SENTRI, FAST. We have our Western Hemisphere Travel Initiative requirement for a card that would allow for border crossings. We have potential Registered Traveler Programs domestically and internationally. There are a multiplicity of biometrically-enabled cards that are contemplated for the transportation and overall security world, which we hope to be able to bring together. I'll give you just one example of how we do that administratively as we're intending to create a common area for appeals, one common place so that we can have the most efficient and customer-friendly place to go to get problems cleared for these kind of cards if there's a concern, a question, or an issue about background clearance.

The CHAIRMAN. Well, we've got a little problem at the floor right now with an immigration bill. A lot of the people here, are they going to be involved in immigration issues?

Mr. JACKSON. The idea is that we would use this same set of tools and capabilities. If, as the President has requested, the Congress approves a temporary worker program, it would require the same type of biometrically-enabled card, so the same essential data architecture that we are using for TWIC will be a precursor for how we could handle what would be a large inflow of background investigation and card issuance that would have to be associated with that program. Yes, sir, we are trying to align this multiplicity of unaligned programs and tools as best we can and as fast as we can.

The CHAIRMAN. I think we know it's an enormous problem, but there have also been enormous delays. We started this in 2001, as I said in my opening statement. And now we're approaching midpoint in 2006. Are we on top of any of the problems that have caused the delays in the past?

Mr. JACKSON. I think we are, sir. The—I'm going to say two things. I want to just state up front that I share your frustration, and I may have kicked your frustration up a notch internally inside the Department. I think that we have taken too long to get this done. We're committing to you to make this a priority. We believe we have cut through issues necessary to get there. We have requested a little bit of flexibility recently from our appropriators to do some reprogramming necessary to make this work. But we're going to make this a priority. We share your sense that it's taken too long.

I will say, in the defense column, this has been more complex, due to the proliferation of technologies and standard-setting processes that are underway. We have tried to align this with the Federal Information Processing Standard, the so-called FIPS–201. There's a government-wide smart-card standard-setting process

which will be completed this year, and which will drive this same type of technology for access to Federal facilities. And what we wanted to do is make sure that, as we created this massive TWIC deployment here, and then subsequently in other modes, that we were aligned with what the Federal Government was doing. We are similarly aligned with a Presidential Directive under HSPD–12, Homeland Security Presidential Directive 12, that sets requirements for biometric and technology standards associated with this world of activity.

So, we are trying to get the whole Federal Government's programs that are doing similar things into a technical alignment. That took some not considerable—a considerable amount of work.

Then we have tried to work with ports and the industry to make sure that we are not big-sticking them and not understanding their business operational needs in this—and requirements—for making this work well, so that we do not cause their businesses to implode. We are committed, on an ongoing basis, to continuing that dialogue. That has eaten up some time.

I'm telling you that, despite those issues, we could have, and should have, moved faster. I will concede that to you. But we are moving at a forced march right now, and we're not going to let up.

The CHAIRMAN. Well, then, last, let me ask you probably an unfair question. Did you explore the concept of having a private firm take on this whole thing and be an agency to produce the proof that is needed in all these areas, whether it's Hazmat or this TWIC or other areas like the traveler card would be?

Mr. JACKSON. The——

The CHAIRMAN. It does seem to me that each agency is going to be going through this same process, and yet there ought to be some area out there where they have people who have the experience and know-how that could take on the job. It looks like the amount paid for the card would pay for that service. Am I wrong?

Mr. JACKSON. It is not an unfair question at all, and we have looked very closely at this. And I will tell you, it is around the nexus of the issues you just raised that we have made some fundamental changes under Secretary Chertoff's direction in how we will implement this program. We had, I'm going to say, earlier at the Department, a more government-centric concept of operations of how this would work. In this model that we have published our regulations to implement, and which we will be soliciting outside industry support to help integrate, we have a better partnership that leverages the capabilities.

And I might just take 1 minute to walk through what this looks like. We have to go around to 300-plus ports and find locations to set up intake systems. We have to find space. We have to go in and enroll individuals. And, for this purpose, we will have an outsourced contract. We'll be in a partnership to make sure that the firm finds real estate, sets this up. It's——

The CHAIRMAN. Why don't you just turn it over to a private firm to do it?

Mr. JACKSON. That's exactly what we're doing, sir. We're contracting that out.

The CHAIRMAN. But you're saying, "We've got to find these spaces."

Mr. JACKSON. We don't. We're giving that to the private sector to do that job. So, then we'll work with them to take the data and manage it through the process of approval. Some of that is inherently governmental. Making the nexus between the FBI data, the criminal history record checks, there is an inherently governmental component to this operation. We're going to outsource a substantial amount of this work in close partnership that allows us to protect privacy, to manage the program, and to get the results.

The CHAIRMAN. Thank you.

Senator Inouye?

Senator INOUYE. Mr. Secretary, if I may, I'd like to follow-up on the questioning by the Chairman.

Last evening, the President addressed the Nation on the immigration problem, and he set forth as one of his elements there that he will have a biometric-type identification system which is foolproof to counter the large amount of counterfeit cards that are being produced. And when I read your testimony, I thought, "I think the President's got troubles here," because your agency awarded, to BearingPoint, this contract, and the pilot program contract was set forth to include 75,000 workers at a cost of $12.3 million. However, it ended up with 1,657 cards, costing $22.8 million. That's what we have received from your agency. This project was over-budget, under-subscribed. But you seem to suggest that this was a very successful pilot program, even if only 1,657 cards were used. Can you tell us why?

Mr. JACKSON. We did issue a larger number than that. The number that I've been told is about 4,000, but it was intended, in Florida, in the Delaware River Basin area, and in the L.A./Long Beach area, to be a more restricted pilot so that we could get an experience with the technology.

We, unlike the deployment, where it will be a fee-based system—in other words, the people who get the cards pay the cost of the cards—this pilot was a totally government-funded exercise to help us understand the problems and complexities of doing this in the field. And it was also an exercise that required building the backroom technical operating platform to manage the distribution of those cards, to pass off the clearances to the multiple Federal agencies that would have to pass on the suitability of a candidate. So, we were building a backbone and a technical architecture to help manage the larger deployment. That was what the BearingPoint contract was, in part, intended to support.

Senator INOUYE. Was the budget doubled?

Mr. JACKSON. I'm sorry?

Senator INOUYE. Was the cost doubled?

Mr. JACKSON. The cost was—I believe that we have spent about—on—total on this to date, about $61 million through 2005. We have about another, I believe, $4.6 million in the budget this year. So, as we move forward, this becomes a fee-based driven system, and the deployment will be paid for based upon the charge associated with purchasing a TWIC card.

Senator INOUYE. Under this cost arrangement, what do you think it will cost to produce 2 million biometric identification cards for immigrant workers?

Mr. JACKSON. We have not done a cost estimate on the immigrant worker program, on the temporary worker program. I can give you a comparison in this area for port workers, and it will be a slightly different type of background investigation, and certainly a different distribution model in how we handle the distribution. But for the TWIC card, there is a preliminary estimate, as part of our regulatory process, that says about $139 for a TWIC card.

Senator INOUYE. Well, how does it compare with the pilot project?

Mr. JACKSON. The pilot project, we didn't charge individuals for the card. We covered the whole cost as a start-up program in the Federal Government out of a Federal appropriation.

Senator INOUYE. That cost about $25 million for 4,000 cards?

Mr. JACKSON. I can get the—I can get the numbers for you, sir, to be more specific.

Senator INOUYE. I'm concerned, because eventually this committee will have to come up with numbers that the people of the United States can understand.

Mr. JACKSON. As we roll-out—if we were to do the temporary worker program, which the Department strongly supports and the President strongly supports, we would have an economy of scale here that would allow us, we think, to drop the cost of the card production part of that equation down. There has been a variety of conversations about fees, fines, registration, others associated with the immigration bill's look at temporary workers that would be funneled into the fee issue, as well as the cost of production.

Senator INOUYE. The Chairman is from Alaska, and I'm from Hawaii. And so, the Merchant Mariner Document, MMD, is very important to us. Now you have your TWIC program, and the Coast Guard is involved in the Merchant Mariner Document. Right now, we need more seamen. Is there going to be a mix-up or some seamless process whereby we won't have to take 6 weeks or 8 weeks to issue a card?

Mr. JACKSON. Yes, sir. We will make this a seamless integration. And this is part of what the aligned rulemaking of the Coast Guard and the TSA seeks to accomplish. Right now, there are several credentials—the Merchant Marine Document, the license, the Certificate of Registry, and the Standards Training Certification for Watchkeeping—everything has an acronym, the so-called STCW endorsement. These are credentials. And what the Coast Guard has proposed is one Maritime Mariner Document which would allow us to take the work that we've done to issue these certifications and issue an actual biometric identifier. And the TWIC is that identifier. So, the Coast Guard, right now, has, I'm going to say, a little bit more burdensome process. They have, I believe, 17 processing centers that mariners have to go to. What we would be able to do is allow mariners to go to a broader swath of intake facilities that will be operating on a permanent basis as TWIC continues and to complete their enrollment in an integrated fashion. This would give them unescorted access to port facilities, and it would allow the Coast Guard to add those certifications, qualifications, and standards proof that they need to that document.

Senator INOUYE. You've indicated that it is very difficult to have a name-based background check. And how much easier is fingerprint background checks?

Mr. JACKSON. What we're doing is, we're combining both name and fingerprint-based background checks. What we have done to begin to get a start on the ramping-up of security in ports is to work through a process of managing name-based record checks prior to the actual distribution of TWIC cards in ports around the country. This, we estimate, is—some 400,000 individuals would go through this process. We've got a notice on the table, and the industry is required, by early next month, to have the names back. We're already receiving names. We've done a pilot program of testing names for this. And what this allows us, basically, to do is check citizenship status and whether or not the individual is on the terrorist watch list or on a terrorist list that we're concerned about.

So, that is a—I'm going to say, a—an early installment on trying to improve the security associated with individuals moving in and out of port facilities. And that's underway. And we expect that to be completed for that first population pool this summer.

Senator INOUYE. Well, I wish you the very best, sir.

Mr. JACKSON. Sir, it's a complex task, but we're committed to making it work, and we appreciate the support that you've given us to keep our feet to the fire.

The CHAIRMAN. Senator Pryor?

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

Let me, if I may, Secretary Jackson, follow up on what Senator Stevens, and Senator Inouye have been asking about, and that is, I'm a little confused, I guess, on why it looks like we're heading down the path of having both the TWIC program and also the HME, the Hazmat program. It seems that both have identical security assessment and disqualifying offenses. Why have both?

Mr. JACKSON. The hazard materials certificate requirement compels individuals who drive trucks with hazardous materials to go through this background review. But not all people who enter a port drive hazardous materials and, therefore, have that certification.

Senator PRYOR. But don't they have the identical factors that you look at for both?

Mr. JACKSON. We are substantially aligning these two. And, in fact, you're absolutely on point, sir, we are actually going to give a discount to people who have a current hazardous material certification so that we will not have to repeat the work that we've done to check their background, to check the watch list. The work that's been done for them will be retained, leveraged, and integrated to this program so that if you've been through that process, you have a lower cost. But, in this case, we're actually giving you a credential, rather than a certification for your driver's license, that you're—that you have a hazardous material certification. So, you now have this card, biometrically-enabled, capturing your fingerprints, that would allow you to enter a port. It's also the case that many truckers who do access work in and out of ports on an

unescorted basis will need these, in addition to truck drivers who have had the hazardous materials. So, we have some hazardous material drivers who never go in a port, they need this program of their own; others who are entering into the port terminal who don't drive Hazmat, will need the TWIC, as well.

Senator PRYOR. To me, it just seems duplicative to do it that way, because when you have a—you know, these truck drivers, they get certified on a lot of different things that they don't really use, and it seems to me it would be better to streamline and have one, but we can talk about that——

Mr. JACKSON. I think, sir, you're right. And the answer is, we're streamlining it into TWIC. TWIC is the card——

Senator PRYOR. All right. That's——

Mr. JACKSON.—and——

Senator PRYOR.—what I was asking.

Mr. JACKSON.—Hazmat was a precursor to having a fully functioning Transportation Worker Identification Card that can be multimodal in its nature.

Senator PRYOR. At one point, I think we were told that TSA wasn't keeping fingerprints. Now I think you're saying that they are keeping fingerprints. Is that right?

Mr. JACKSON. Yes, sir.

Senator PRYOR. And, here again, is this something that is used in both credentials, for the HME and the TWIC, right now?

Mr. JACKSON. At the intake part for both processes, we capture fingerprints.

Senator PRYOR. And so, I think what you said a few moments ago is, it makes sense that if you capture it once, you don't have to do it again.

Mr. JACKSON. Precisely.

Senator PRYOR. Right.

Mr. JACKSON. Yes, sir.

Senator PRYOR. OK. And what about—I know what we're focused on, obviously, U.S. drivers, U.S. ports, et cetera, transportation workers—what about—do we—are we doing anything internationally to look at what they're doing around the world to see if we're close to having the same standards?

Mr. JACKSON. We are talking—I was at a European Union meeting last week, and this topic came up as a topic of discussion for exchange. We, as a matter of fact, have a visiting official from the EU at DHS today to continue to look at some of our issues associated with the documentation requirements and security requirements for cross-border travel. So, we do talk a lot with other nations about their best practices.

On this score, in particular, we will be very engaged with both Canada and Mexico about the prospect, for example, that a Canadian truck driver may wish to come and access a U.S. port. And so, we're very much open to having a TWIC card that could accommodate that reality, and we want to work our way through comparable security processes to make it work.

Senator PRYOR. All right. Let me ask one more question about the expense of this. And I do have some questions that I'll submit for the record, with the Chairman's permission.

But let me ask about the expense of this. Right now, the trucking company—or maybe technically the driver—but the trucking company bears the cost of getting these certifications, et cetera. I have a concern that that may hurt the smaller trucking companies. It probably won't hurt the big guys, but it may hurt the smaller trucking companies. Just as a matter of policy, is it better to put the burden, the cost, on the trucking companies and drivers, or is it better for the government to pay for this? And the reason I say that, we're talking about general public safety, and—why are we having those people, who are hauling materials, picking up, dropping off materials—why are we having them pay for it? Why not the taxpayer, at large?

Mr. JACKSON. It's a cost of doing business, and we believe it's appropriately placed on the business community to do this. It's also been authorized by Congress for us to collect the fees. It would be a very large sum of money for us to set out as a government subsidy to pay for this. And we believe that this is a—an equitable way to get a security enhancement in the port environment, and the fastest way to get it done.

Senator PRYOR. That's fair enough.

The CHAIRMAN. Just one last question. I'm not sure about the fee that you've proposed in this proposed rulemaking. Does the fee that you've indicated there cover the complete cost of enrollment, the threat assessment credential production and delivery? For instance, does it cover the cost of the card readers and the other things that each port will have to have?

Mr. JACKSON. No, sir, it does not cover the cost of the port-centric infrastructure. I will tell you that that will be a subject of a subsequent rulemaking, to walk through the technologies that would be needed to do fingerprint capture upon presentation of credentials at a gate or at a facility. So, we are working this in a two-step process. First we're going to get the cards issued. It'll be a biometric photo and have biometric capabilities. But we will not immediately, in a given port, impose a requirement that there be readers in every private terminal and at every gate to manage this. That will be a process that the Captain of the Port, with the Coast Guard's strong engagement here with the industry, will work through, a plan and a time-table, which will be done on a port-by-port basis, is the current thinking. And that will follow in the relatively near-term, after the issuance of cards at each of these facilities. So, it's a two-step process.

The CHAIRMAN. Well, back in the days when it was proposed that every gun owner have identification in order to purchase ammunition, et cetera, we went through this process and determined, at the time, that the least expensive process would be to issue a card with a number on it, and that would be presented like a credit card to a dealer, and they'd just run it through the card reader, and the FBI system would respond with a photo, et cetera, of the person who had that card. Now, that whole idea was rejected, but that was one of the things we looked into.

Why haven't we looked at the idea that everyone gets a card, and there's a central identification system that you access, just like a credit card?

Mr. JACKSON. Well, there's a combination of central and distributed systems in this TWIC model that is centralized in the approval and the continuous checking against updated terrorist watch lists. So, you get approved, it goes through a central switch. It's a governmental—inherently governmental function to look at some of these lists. You are issued a card. The sheer volume of in-and-out transactions would mitigate against having a real-time check each time you did this. So, what we do is, we take an authorize list of TWIC participants and download that to the facilities that need the access. It also allows us to be able to authorize, ultimately, access to multiple port facilities in multiple ports for a single TWIC card.

So, it's a combination of centralized function and speed. The speed of actually being able to read one of these cards and move in and out is something on the order of a third of a second in our field tests. So, we need that high throughput, high volume. We're talking about roughly 750,000 TWIC cards in the maritime world that would go out and be used on a daily basis in a high volume.

The CHAIRMAN. Thank you very much. Any further questions, gentlemen?

[No response.]

The CHAIRMAN. We very much appreciate your appearance here today and look forward to working with you on the overall problem.

Mr. JACKSON. My pleasure. Thank you, Mr. Chairman.

The CHAIRMAN. Our next panel is Mr. George Cummings, the Director of Homeland Security at the Port of Los Angeles; Ms. Lisa Himber, Vice President of the Maritime Exchange for the Delaware River and Bay; and Mr. Larry Willis, General Counsel of Transportation Trades Department of AFL–CIO.

[Pause.]

The CHAIRMAN. Good morning. We thank you very much for coming. If it's agreeable, we'll just call on the witnesses in the order that I've introduced them.

Mr. Cummings, I appreciate your being here and look forward to your testimony.

All of your statements will be printed in the record in full. We'd appreciate it, if you could, to summarize them, to some extent. We will have another vote here on the floor of the Senate in 40 minutes.

Thank you very much.

STATEMENT OF GEORGE P. CUMMINGS, DIRECTOR OF HOMELAND SECURITY, PORT OF LOS ANGELES, CITY OF LOS ANGELES HARBOR DEPARTMENT

Mr. CUMMINGS. Good morning, Mr. Chairman and members of the Committee, and thank you for inviting the Port of Los Angeles to testify before you today to share the port's perspective on the National Transportation Worker Identification Credential Program and to convey our experience in our participation in the test and prototype phases of the program.

I'm George Cummings. I'm the Director of Homeland Security for the Port of Los Angeles, which is the Harbor Department of the City of Los Angeles.

Port security is a top priority for the Port of Los Angeles. The port is not only responsible for the security and well-being of our

tenants, workers, visitors, and the surrounding communities, we must also maintain the free flow of commerce that moves through our port and is vital to the Nation's economy.

As you're aware, Mr. Chairman, more than 95 percent of the U.S. overseas trade moves through the Nation's seaports. The Port of Los Angeles, combined with the Port of Long Beach, handle more than 43 percent of the Nation's containerized commerce. In addition to containerized freight, these ports also handle millions of cruise and ferry passengers, automobiles, and we handle over 50 percent of California's oil.

Following the tragic events of September 11, 2001, Congress enacted the Maritime Transportation Security Act. The U.S. Coast Guard rapidly developed regulations to establish security standards for port facilities. All 50 of the maritime facilities within the Los Angeles/Long Beach Port complex were in compliance with these regulations by the July 1, 2004, deadline.

Full compliance with these new security standards achieved an important milestone; however, comprehensive credentialing programs, such as the TWIC program, are an essential part of security for our Nation's seaports and has not yet been fully realized.

The Los Angeles/Long Beach Port complex, along with Delaware River and the State of Florida, participated in the two developmental phases of the TWIC program. Our experience during the phases of the—of this—development of this program taught us several lessons. We would like to share a few of these with you today.

First, Mr. Chairman, the card-reader systems must be based on the best available technology and must use a biometric to—the biometric capability to prevent unauthorized access to terminals.

The issuance of the credential must be based on a background check that will effectively eliminate individuals that could pose a security risk.

The program needs to include fair and accessible appeal and waiver processes available to individuals who are initially found ineligible for the card.

The regulated facilities must maintain the authority to grant access only to those individuals that they determine require unescorted access to their individual facilities.

The regulated facilities must be afforded flexibility on how they set up the systems on their individual terminals.

Last, costs associated with the program must be reasonable, both costs to individuals that require a card, as well as costs associated with system installation and maintenance on the facilities.

As you're aware, Mr. Chairman, the TWIC program has been in development for several years, and implementation of this program remains a critical element of security for our Nation's seaports. The Port of Los Angeles is encouraged with the recent Federal notice of proposed rulemaking regarding the TWIC program. We look forward to participating in an expedient regulatory development process.

In closing, Mr. Chairman and members of the Committee, we thank you for your leadership in calling attention to the most critical parts of port security, and one that has not yet been fully accomplished. Thank you, again, for the opportunity to participate in this hearing. I look forward to any questions you may have.

[The prepared statement of Mr. Cummings follows:]

PREPARED STATEMENT OF GEORGE P. CUMMINGS, DIRECTOR OF HOMELAND SECURITY, PORT OF LOS ANGELES, CITY OF LOS ANGELES HARBOR DEPARTMENT

Good morning, Mr. Chairman, and members of the Committee. Thank you for inviting the Port of Los Angeles to testify before you today to share the port's perspective on the national Transportation Worker Identification Credential (TWIC) program, and to convey our experience as a participating Port during the test and prototype phases of the TWIC program.

I'm George Cummings, Director of Homeland Security, for the Port of Los Angeles. I'm responsible for coordination of the Port's homeland security and maritime security programs at the national, state, and local levels.

Port security is the top priority for the Port of Los Angeles. The Port is not only responsible for the security and well-being of our tenants, workers, visitors, and the surrounding communities; but we must also maintain the free flow of commerce through our Port which is so vital to this Nation's economy.

The Importance of Maritime Trade and Ports

As you are aware, Mr. Chairman, more than 95 percent of U.S. overseas trade moves through our seaports. As a premiere port of entry for cargo on the West Coast, the Port of Los Angeles occupies 7,500 acres of land and water along 43 miles of waterfront. Together with our San Pedro Bay neighbor, the Port of Long Beach, we handle more than 43 percent of the Nation's containerized commerce. That translates to 7.5 million twenty-foot equivalent units of containers that entered the Port of Los Angeles in 2005. With the Port of Long Beach, a total of 14.3 million twenty-foot equivalent units of containers entered the San Pedro Bay Port complex. Together, we rank the fifth busiest port complex in the world. Alone, the Port of Los Angeles is the eighth largest container port in the world, and number one in the United States. In addition to containerized freight, the Los Angeles/Long Beach Port complex handles over one million cruise passengers, half a million autos, and over 50 percent of California's oil.

Trade through the Port of Los Angeles has grown steadily by an estimated 20 percent each year over the last 5 years, and we expect this trend to continue. Likewise, the industry expects national maritime trade volumes to double by the year 2020, although some economists have predicted that such doubling may occur as early as 2014 due to the demands of the American marketplace.

In the event of an unforeseeable incident, whether caused by intentional acts or natural disaster, it is the Port's responsibility to resume cargo operations as quickly as possible in order to minimize any impact to the Nation's economy that is dependant on trade and the movement of goods.

A recent example of the effects of a major port shutdown occurred in the Fall of 2002 when a labor disruption caused a 10-day shutdown of the West Coast ports that brought cargo movement to an immediate halt. This action cost the Nation's economy an estimated $1.5 billion a day (valued in 2002 dollars), disrupting the availability of goods and products that Americans rely upon daily. A healthy U.S. economy relies heavily on secure, functioning ports throughout the United States.

Maritime Transportation Security Act Regulations

Following the tragic events of September 11, 2001, Congress enacted the Maritime Transportation Security Act (MTSA) of 2002. Section 102 requires background checks and the issuance of biometric transportation security cards for all maritime personnel who need access to secured areas of ships and port facilities. As such, the U.S. Coast Guard rapidly developed regulations to establish security standards for port facilities. The MTSA regulations required terminal operators to submit their facility security plans by December 31, 2003, and the deadline for implementation was July 1, 2004. All 50 of the maritime facilities within the Los Angeles/Long Beach Port complex—cargo terminals, liquid bulk and dry bulk terminals, and the World Cruise Center were in compliance by the July 1, 2004, deadline. Full compliance with the new security standards achieved an important milestone; however, complete implementation of the TWIC program is essential for the security of the Nation's seaports.

The Importance of Access Control and Credentialing

Access control at ports and port facilities is a critical component of port security, and access control will require a comprehensive credentialing program. The Los Angeles/Long Beach Port complex, along with the Delaware River and the State of Florida, participated in the two developmental phases of the TWIC program. We

consider a Federal credentialing program, such as TWIC, to be the solution to this major security challenge. We fully support the TWIC program and look forward to its full implementation. Ports throughout the Nation are waiting for the TWIC program guidance before they can fully complete their access control systems.

Critical Elements of the TWIC Program

The Port's experience during the TWIC test and prototype phases showed us several critical elements of the program that we believe must be addressed in the fully implemented program. The Port recommends that the following elements be incorporated into the TWIC program:

1. The card and reader systems must be based on the best available technology using biometrics to prevent unauthorized access;
2. The issuance of a credential must be based on a background check that will effectively eliminate individuals that would pose a security risk;
3. The program needs to include a fair and accessible appeal and waiver process for individuals who are initially found ineligible for a TWIC card;
4. The regulated facilities must maintain the authority to grant access only to those TWIC holders that require access to that facility;
5. The regulated facilities must be provided with an electronic connection to the Federal agency operating the national database to readily verify the validity of TWIC cards presented at their facilities;
6. The regulated facilities must be afforded flexibility on how to set up the TWIC access control systems for their facilities; and
7. Costs associated with the program must be reasonable, including costs to the individuals who require TWIC cards, as well as costs associated with card reader system installation and maintenance.

The Need for Expediency

As you are aware, Mr. Chairman, the TWIC program has been in development for several years, and implementation of a robust credentialing program at maritime facilities remains critical to securing our Nation's ports. The recent Federal Notice of Proposed Rulemaking encourages the Port of Los Angeles that there will be an expeditious regulation and implementation process for TWIC, and we look forward to participating in that process.

Closing

In closing, we thank you for your leadership in calling attention to one of the most critical elements of port security, and one that has not yet been fully accomplished—the TWIC program. Also, we appreciate the opportunity to share the Port of Los Angeles's experience with the TWIC test and prototype phases. The Port is confident that the Federal regulatory development process will occur as quickly as possible leading to the full implementation of the TWIC program. Thank you again for the opportunity to participate in this important hearing, and I look forward to answering any questions you may have.

The CHAIRMAN. Thank you very much, Mr. Cummings.
Ms. Himber?

STATEMENT OF LISA B. HIMBER, VICE PRESIDENT, MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY; VICE-CHAIR, NATIONAL MARITIME SECURITY ADVISORY COMMITTEE (NMSAC)

Ms. HIMBER. Good morning, Mr. Chairman and members of the Committee. My name is Lisa Himber, and I am Vice President of the Maritime Exchange for the Delaware River and Bay. I also serve as Vice-Chair of the National Maritime Security Advisory Committee.

Today I was specifically asked to talk about any delays that I think might have prevented TSA from launching this program. But before I get into that, let me start by saying that despite the ongoing delays, we continue to strongly support the TWIC program.

By way of background, the Maritime Exchange was asked to be TSA's partner on the East Coast pilot project, given the work that we had previously accomplished in integrating what we were calling a Regional Delaware River ID System into our existing Maritime Online Ship, Cargo, and Crew Manifesting System.

In the planning phase of the TWIC pilot program, we found TSA was very effective. They visited a variety of port stakeholders and were, thus, able to understand a full range of security needs. And, most importantly, TSA communicated openly and frequently with maritime stakeholders during this process.

From the initial planning effort, TSA developed what we thought would be an effective blueprint to move the project forward in May of 2003. At that time, the expectation remained that the Technology Evaluation and Prototype phases would follow directly, and the pilot program would be completed by December of 2003.

The Technology Evaluation phase ended in October of 2003 only slightly behind schedule. However, for reasons that were never made entirely clear to us, the Prototype phase of the East Coast program did not kick off until November of 2004. Among the reasons we heard included the fact that the Technology Evaluation report took longer to review than expected; thus, delaying the issuance of the request for proposals and contract award for the Prototype phase. There also appeared to have been a lengthy delay in the Fall of 2004 associated with a contract modification.

The Maritime Exchange office was the first East Coast site installed, which launched on November 17, 2004. Unfortunately, the enrollment at our site did not go as well as expected. Card issuance was delayed, for a variety of reasons. Data was not correctly entered into the system, data was missing, the system lost communication with the central server, et cetera. Whether these were purely technical issues or less—lack of trusted agent training, at this point, we don't know.

Though the pilot program was scheduled to end on June 30, 2005, card production did not begin in earnest until the summer of that year. Some of the technical setbacks that we understand included problems with the employees' sponsor worksheet, the TWIC web portal, and the lengthy delay associated with moving the card production facility in the middle of the program. Other concerns expressed were poor communications between the trusted agents and the pilot site locations. Because of the ongoing delays, we were pleased that TSA continued to support the East Coast locations well beyond the official program conclusion.

In addition to the technical problems, we believe there were administrative and operational issues, as well. Foremost among these must be the high turnover at all levels within DHS, TSA, the TWIC program office, and the contractors. We also believe that the discussions which took place during this period about whether TSA should issue a standard or manage the program served to delay the process significantly.

In December of 2005, the Maritime Exchange requested a copy of the prototype evaluation report, but this request was declined. Then, in February of this past year—of this year—TSA informed the National Maritime Security Advisory Committee that the

TWIC regulations had been completed and approved by Coast Guard and TSA, and were awaiting final approval.

With the release of the draft notice of proposed rulemaking last week, many of the questions surrounding the implementation of TWIC had been answered. The deployment schedule, however, remains the most pressing question. Of equal concern is the ability of DHS to put together a team of individuals who will be able to lead the project through to its completion. And, also, it will only be upon formal publication of the rulemaking that we will be able to engage in the public debate surrounding the background check.

There are other questions and concerns, and some of these are listed in my written statement.

In closing, let me say that all the preceding notwithstanding, we believe TSA has assembled the basic building blocks of a program which will meet the need to validate individuals seeking access to secure maritime facilities, and we look forward to continuing to work with DHS to ensure that TWIC will be deployed in the safest, most secure, and efficient manner possible.

This concludes my remarks, and I thank you for the——

The CHAIRMAN. Thank you——

Ms. HIMBER.—opportunity to speak.

The CHAIRMAN.—Ms. Himber.

[The prepared statement of Ms. Himber follows:]

PREPARED STATEMENT OF LISA B. HIMBER, VICE PRESIDENT, MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY; VICE-CHAIR, NATIONAL MARITIME SECURITY ADVISORY COMMITTEE (NMSAC)

Good morning, Mr. Chairman and members of the Committee, and thank you for the opportunity to present testimony today. My name is Lisa Himber, and I am Vice President of the Maritime Exchange for the Delaware River and Bay. The Maritime Exchange is a nonprofit trade association representing the members of the commercial maritime industry in Southern New Jersey, Southeastern Pennsylvania, and Delaware. Our mission is to promote the safety, security, economic viability and environmental health of the Delaware River Port complex. Included among our 300 members are those companies and individuals on the front lines of the international border of the port—such as port authorities and private terminal operators, tug and barge companies, labor organizations, vessel operators and steamship agents, just to name a few.

In addition, I serve as Vice-Chair of the National Maritime Security Advisory Committee (NMSAC), which as you as you are aware was established under the Maritime Transportation Security Act (MTSA) of 2002. I, and my fellow NMSAC members, are charged to provide advice to the Secretary of the Department of Homeland Security on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and security concerns of the maritime transportation industry.

I appreciate this opportunity to discuss the state of the Transportation Worker Identification Credential (TWIC) program, issues which may have prevented TSA from launching this program from a pilot participant perspective, and its future implementation. The TWIC program has been one of the priority Federal projects for my organization and its members in the Delaware River maritime community since even before its official inception.

Background

The Exchange role in the port—Like most trade associations, the Maritime Exchange is an advocate on issues of concern to its members. However, what sets the Exchange apart is its day-to-day operating role in the port. The Maritime Exchange operates on a 24/7 basis and one of its key responsibilities is to collect, store and disseminate schedule information on all commercial cargo ships arriving or departing the Delaware River. We also serve as a communication and information hub for the tri-state port, distributing messages between ships and their shoreside service

providers as well as distributing Federal safety, security, operational, and procedural bulletins to the maritime businesses operating throughout the region.

In addition to our traditional Ship Reporting function, which dates back to 1875, in the mid-1980s the Exchange began the development of what is now known as Maritime On-Line (MOL). This system is a community-based information network which provides a mechanism not only to obtain anticipated, current and historical vessel movement information but also offers a tool for steamship carriers and their agents to submit cargo manifest data to U.S. Customs and Border Protection and advance electronic notice of vessel arrival and departure information to the U.S. Coast Guard. Through MOL, the Exchange provides Delaware River port operators with a cost-effective means to both comply with Federal information reporting requirements as well as to share information, such as manifest data or cargo release status, with local partners in the transportation chain through a central community maritime database system.

Development of a regional standard ID—As Maritime On-Line had become a useful tool for doing business at regional ports, and because the Exchange had demonstrated its ability to bring together the various partners in the maritime industry to develop, implement, and use a community information system, several Exchange members approached us in the late 1990s to discuss the feasibility of developing a system under Maritime On-Line which could be used to identify truck drivers accessing the various cargo facilities in the three states.

The Exchange organized a working group of system users—terminal operators, truck drivers, brokers and freight forwarders, steamship agents—and identified the requirements of what would be known as the Electronic Driver Identification (EDID) System. By September of 2001, the system design was complete, and the Exchange was working to identify a means of funding the initial program development. The premise behind this system was a centralized database and the issuance of an ID card that would be accepted at all participating Delaware River maritime terminals.

Immediately after the events of September 11, 2001, Exchange members asked whether the system we had designed to identify truck drivers could be expanded to include anyone requiring access to maritime facilities. Like truck drivers in the State of Florida, those doing business in the Delaware River were required to obtain multiple identification cards, and the maritime community agreed that development of a single, standard ID card would be a critical program under new heightened security programs at maritime facilities.

As a result, by October of 2001, the Exchange had identified funding to develop a pilot program, and in partnership with the Port of Wilmington, Delaware, had successfully programmed and tested what would become the Delaware River ID (DRID) system by January of 2002. We subsequently received a Port Security grant to continue this program.

It was because of this effort that the agency which would become the Transportation Security Administration (TSA) selected the Delaware River as one of the TWIC pilot program locations. Among the rationale behind this selection was the fact that if such a system could work effectively at Delaware River ports, with three states and multiple private and public port facilities, it would work at all U.S. ports.

TWIC Pilot Program

Having been involved in the TWIC program even prior to the establishment of the TSA and the August 2002 launch of the East Coast TWIC pilot project, my organization and its members have been keenly interested in the successful deployment of this program.

The importance of TWIC to the maritime industry is underscored by the fact that the full NMSAC membership—which includes a diverse cross-section of maritime stakeholders—unanimously concluded that TWIC is among the most important components of the national maritime security effort. As a result members elected to make TWIC the number one priority on the NMSAC agenda. Last May, the Committee presented DHS with a full set of recommendations for TWIC implementation. We are pleased to see from the draft Notice of Proposed Rulemaking that most of the NMSAC recommendations have been adopted.

Despite the many problems with TWIC over the last several years, we continue to support the idea of a standardized credential to be used at U.S. seaports. In the first phase of the TWIC program, the Planning Phase, TSA did everything right. They visited with a variety of operators at differing types of ports and were thus able to understand the full range of security needs. And they talked with the people who require access to multiple facilities—including pilots and other mariners, steamship operators, trucking companies, vendors and labor—and they met with other local Federal, state and municipal agencies to better understand their needs

and concerns. And most importantly, TSA communicated openly and frequently with maritime stakeholders during this process. During the Planning Phase of the program, TWIC program staff kept us apprised not only of their progress, but when there were setbacks, TSA explained the reasons and provided stakeholders with the opportunity to provide input into the program development process and assistance in overcoming obstacles.

From that effort, TSA developed what we thought would be an effective plan to move the project forward. That was in May of 2003. At that time, the expectation remained that phases two and three of the program, the Technology Evaluation and Prototype phases, would follow immediately, and the pilot program would be completed by December of 2003.

The Technology Evaluation phase ended in October of 2003, slightly behind schedule, and for the most part, we believe it achieved its goals; that is, TSA could issue cards which could be read by scanners at various facilities. At the end of the evaluation TSA determined that the TWIC would need to utilize a variety of technologies—such as smart chip, magnetic stripe and bar code—in order to meet its key mandates: TWIC must be able to integrate seamlessly with facilities' legacy systems to minimize costs and facilitate rapid program deployment; and it must be interoperable among all private and public port facilities.

During the Prototype Phase, TSA and stakeholders were to test the implementation of the technologies identified in phase two, as well as the host of business processes associated with implementing the TWIC program. These included trusted agent training, card application, threat assessment, card production and issuance, revocation, hot-listing, replacement, use of a biometric, and the electronic communications between terminal facilities and the central database. For reasons which were never made entirely clear to pilot program participants, the Prototype Phase of the East Coast pilot program did not officially begin until November of 2004. We know that the Request for Proposals was not released until May of 2004, and the contract was not awarded until October of that year. Some of the reasons cited for the delay included the fact that the Technology Evaluation report took longer to review than expected, thus delaying the development and release of the Request for Proposals. There appeared to have been a lengthy delay in the Fall of 2004 resulting from a subsequent modification to the contract once it had been awarded. Finally, the fact that the contractor selected for phase three was not the same as that used for phase two undoubtedly contributed to the delay.

The Maritime Exchange office was the first East Coast site installed for the third phase test. By November 17, 2004, we had pre-enrolled our ten employees, TSA had installed the biometric readers and cameras. Unfortunately, the enrollment at our site did not go as well as expected. Several members of our staff were required to return multiple times to obtain their cards for a variety of reasons—data was not correctly entered into the system, data was missing, the trusted agent lost connection to the central server, the system would not save data after it had been entered, etc. Whether these were purely technical problems or lack of sufficient trusted agent training is unknown.

Though we were certainly surprised by the number of problems encountered, the Exchange was pleased to be the first site—better to work through the glitches at an office location rather than at a working maritime facility where moving people quickly through the gates is paramount.

Similar delays in completing the enrollment site installations and beginning the processes to register applicants were reported by the other pilot participant sites.

Although the pilot program was scheduled to terminate on June 30, 2005, card production did not begin in earnest until well into the summer of that year. Some of the technical setbacks included problems with the employer sponsor spreadsheet (an Excel spreadsheet the employers were to complete and return to TSA to upload into the database in advance of enrollment), problems with the TWIC web portal, system shutdowns for undefined upgrades, and the lengthy delay associated with moving the card production facility from Pennsylvania to Kentucky in the middle of the program. At least one TWIC sponsor was notified that data for several employees was lost during this transition. He was subsequently informed that the data was never lost but rather it had been incorrectly entered. In either event, the individuals were required to re-enroll.

Other concerns expressed during the pilot program were poor communications between the trusted agents and the pilot site locations (*e.g.,* schedule of enrollment at the facilities, failure to notify sites of trusted agent employee turnover, no advance notice of installation work, etc.). The TSA and its contractors did not, for example, consult the Delaware River stakeholders in developing the TWIC web portal. As a result, when it was demonstrated at a stakeholder meeting on March of 2004,

some key functionality was not included, such as the ability of a sponsor to delete an employee from its roles and request card deactivation.

In some cases, cards were not produced until well after the June 30 program termination. As a result, TSA continued to formally sustain the program at the three Delaware River maritime locations through October 31, 2005. We were also pleased that TSA continued to support the Wilmington, Delaware site, albeit on a limited basis, through March 31, 2006.

In addition to the delays resulting from the technical problems, we believe there were administrative and operational issues as well. Foremost among these, of course, must be the high employee turnover at all levels—DHS, TSA, the TWIC program office staff, and the contractors. In addition to the multiple individuals who held the TSA Administrator post during this period, the TWIC Program Manager changed three times, and there were four project leads for the East Coast pilot program between August of 2002 the Fall of 2005. At each instance, the incoming individuals had to be brought up to speed on the program and its participants. Needless to say, there was no clear way to circumvent delays of this nature.

We also believe that the discussion which took place during this period surrounding the question of whether TSA should issue a standard or guideline rather than manage the program served to delay the program significantly.

That being said, in March of 2005, TSA informed the National Maritime Security Advisory Committee that its intentions were to publish a Notice of Proposed Rulemaking by September 2005. During the subsequent months, particularly when it became apparent that the regulation would not be forthcoming in the immediate future, the NMSAC continued to request a response to the recommendations submitted in May of 2005 and to seek an explanation for the ongoing delays.

In December of 2005, my organization requested a copy of the Prototype Phase evaluation report; however this request was denied.

The TSA and Coast Guard did respond to the NMSAC recommendations on February 23, 2006 via a teleconference, the members were not provided with any explanation for the delay. At that time, we were told the draft regulations had been completed and approved by TSA and the Coast Guard and were awaiting final approval from DHS and the Office of Management and Budget.

Moving Forward

With the release of the draft Notice of Proposed Rulemaking on May 10, 2006, and under the assumption that the formal Notice will not be altered substantially, many of the questions surrounding the implementation of the TWIC program have been answered. The program schedule, of course, remains the pressing question. When will the regulation be published in the *Federal Register,* and what is the implementation schedule at the port level?

Of equal concern as we move to transition TWIC from a pilot program to full implementation is the ability of DHS to put together a team of individuals who will be able to lead the program through completion. Needless to say, while the high employee turnover in both the DHS leadership and within the TWIC program office itself caused significant delays during the pilot, the ability to keep the TWIC program moving along a predetermined time-table once implementation begins will be paramount to its ultimate success.

There were very few surprises in the draft Notice. Most of what TSA had indicated to NMSAC and other stakeholders would be in the final rulemaking is in fact included. From our perspective, the draft rule raises few questions relating to the general program implementation. There are, however, questions and concerns about some of the details not included in the draft and how the answers to those questions will affect deployment. These include:

There does not seem to be a provision for casual longshore labor. While we recognize that it is necessary to screen individuals who will require unescorted access to secure areas at maritime facilities, it is equally important that this program does not dramatically and adversely affect commerce.

There has been significant debate during the last few years about the effect the criminal history background check would have on transportation workers. While a number of maritime interests agree that the standards for the TWIC should be consistent with those of the Hazardous Material Endorsement, a significant majority believe that security regimes at maritime facilities do not dictate such stringent requirements. It will only be upon publication of the Rulemaking that we will be in the position to publicly dialogue on this critical issue.

Since foreign vessels and therefore crewmembers are exempt from the regulation, facilities are concerned about how they will grant access to visitors arriving by water.

Under the draft, terminal/vessel operators are required to know who is on board at all times—and to store the information in a database for not less than 2 years—and also that Federal officials and state/local law enforcement are not included in the TWIC requirement. It appears, therefore, that terminal facilities will be required to manually enter information pertaining to those visitors who are exempt from the TWIC requirement. This may not be practical.

In the event of an incident at a facility, is the TWIC program to be deactivated at the affected site to allow access to first responders? Would we want the program deactivated at such a critical time? If not, how would we validate emergency personnel?

Who will be eligible to serve as trusted agents? We believe contractors should not only undergo the same screening as applicants, but they should be held to even higher scrutiny, such as a financial background checks as well as criminal history. In addition, these agents should undergo general business and customer service training as well as TWIC-specific training.

At both initial implementation and beyond, during the interval between application and response, will applicants be allowed continued unescorted access to facilities/vessels if the operators choose to grant such access?

What is the alignment between TWIC and the recently announced Coast Guard screening program for port employees, long-term contractors and longshoremen?

Other more technical concerns include implementation of those business processes which were never tested during the pilot program:

- *Communication with the central database.* The central database would allow facility operators to provide TSA with the names of individuals to whom they grant access. With this feature, if an individual's card were hot-listed, TSA could proactively notify all facilities where the worker had been granted access.
- *Hotlisting.* Since no connection between a central database and the individual facilities was established, the card hotlisting process could not be tested.
- *Interoperability.* One of the original components of the TWIC vision included its ability to be used with legacy systems and across modes. This test was not fully completed. Additionally, because of the delays in implementing TWIC, many vessel and facility operators have been compelled to implement their own programs in order to comply with Coast Guard security requirements and address internal needs. TSA needs to include a mechanism to phase in the use of TWIC so as to avoid the significant and redundant expenses associated with full replacement of legacy systems. Similarly, it is necessary that the final deployment schedule not only allow sufficient time for facilities to purchase and install equipment, but also to modify software to integrate the card reader technology with their internal access control systems.
- *Web portal.* The web portal was designed and tested using an employer sponsor to input and maintain worker data. Under the draft rule, employer sponsorship is not included and applicants will be required to enter and query data individually. How will TSA establish and validate individual accounts?
- *Use of Biometrics.* The prototype did not test use of biometrics with workers at port facilities. This is a significant concern. Also, the draft rule calls for use of an alternate biometric if an applicant is unable to provide the primary biometric. What will this be, and will separate readers be required?

All of the above notwithstanding, we believe TSA has assembled the basic building blocks to launch a program which will meet the need to validate individuals seeking access to secure maritime facilities. And we appreciate that DHS listened to its stakeholders on such key issues as eliminating the employer sponsor requirement, managing the program versus issuing a standard, and aligning the program with other credentials such as the Merchant Mariner Documentation.

Over the years, the maritime sector perhaps more than any other has recognized the need to implement new programs and practices in an effort enhance the security of our homeland. We have dramatically altered business processes and worked closely with DHS agencies to help them achieve their missions. As with many Federal programs, we want to continue to work with TSA on the TWIC program to ensure there are no unintended consequences, such as those which might arise if we are unable to credential casual labor, and that the TWIC will be deployed in the safest, most secure, and efficient manner possible.

We believe that with additional program refinement, the TWIC will ultimately emerge as an invaluable tool to meet the dual goals of improved security and facilitation of commerce.

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

The CHAIRMAN. Mr. Willis?

STATEMENT OF LARRY I. WILLIS, GENERAL COUNSEL, TRANSPORTATION TRADES DEPARTMENT, AFL–CIO

Mr. WILLIS. Thank you, Mr. Chairman.

First I wanted to thank you, again, for the opportunity to testify this morning on the TWIC program, and specifically on its application to port, maritime, rail and related workers.

At the outset, let me clearly state that no one wants to secure our Nation's ports and transportation system more than the workers on the front line. Our members are going to be the first affected if the transportation system is used in an attack—or is attacked itself—so we obviously have a vested interest, as we've articulated many times in front of this committee, to enhancing security.

We also understand that a tamper-resistant TWIC-type card is part of that effort, and we support the stated goals of the program—to identify terrorist security risks and to bar them from having unescorted access to our Nation's ports and other transportation systems. There's no disagreement about that.

But, at the same time, the TWIC program, if it's going to be a success, must strike the right balance. It must enhance security, but it also must protect the legitimate rights of front-line workers. It must include a robust waiver and appeals process. It must protect the privacy of the information, both submitted and generated by the card. It must not burden the individual worker with the cost of this program. And, again, it must focus on identifying genuine, true security risks, and not punish a worker twice for a bad decision made several years ago.

On that point, let me specifically thank this committee for working so hard on the MTSA, and specifically Section 70105, which established the limits and parameters for the maritime security card. You were very clear there. You stated that for felonies only those crimes that cause an individual to be a terrorism security risk should bar that person from the industry. Unfortunately, while that was a good mandate, we think TSA, in issuing the NPRM for this program, for the maritime TWIC program, and, before that, for Hazmat, came up with a list of disqualifying offenses that remains too broad, vague, and, again, not targeted on terrorism security risks.

Let me cite just a couple of examples. Under the TSA's rules, those that commit felonies involving fraud are terrorism security risks. Those that commit crimes of misrepresentation are terrorism security risks. Those crimes involving dishonesty, same thing. These are all bad things. People should be punished. There's no disagreement about that. But does that make an individual a terrorism security risk unworthy to work in a U.S. seaport or unworthy to haul Hazmat?

Yes, TSA did include a waiver in this rule, as they were required to do by this committee. We think that waiver process is extremely important. But that cannot be used as an excuse to include an overly-broad list of crimes.

As you've heard, they will have to check 750,000 workers under this program. This is going to be very complicated. Do we want the

additional burden of having to do waivers for workers who never should have been included in the list in the first place?

So, we would respectfully ask TSA, which we will in our formal comments, and we have been talking to your committee about this—about having TSA, again, take a look at that list of crimes and try to narrow it, try to make it more specific, and try to have it focused on, again, identifying those individuals who are really terrorism security risks.

The waiver process which I referenced, again, is crucial. And for that to have real meaning, it has to have an administrative law judge. We've asked TSA several times for that and that has been denied. I want to thank the Committee for including an ALJ process in its pending Coast Guard bill. That's being held up, obviously, for unrelated reasons. Despite that, we hope and expect TSA will include an ALJ process in its final rule.

We need a national standard with states or local jurisdictions. Having additional background checks that go beyond the list of crimes that's expansive enough in the TSA rule is very problematic. Having those states go forward without a waiver or privacy or an appeals right that's at the Federal level, again, is something that we need to work on. Congress spoke to that in the highway bill for Hazmat. We hope that's carried over to maritime.

The cost of the program has been talked about. As it is included in this NPRM, the costs will be borne by the applicant. We feel that that is unfair. We think the Federal Government has a role to play here in paying for this. And given the fact that workers are going to have to apply for a TWIC, maybe have additional costs for an appeal or waiver, having to pay for the cost of the card is a burden. That's not proper.

I see that my time is up, so I'll stop and be happy to answer any questions the Committee may have.

[The prepared statement of Mr. Willis follows:]

PREPARED STATEMENT OF LARRY I. WILLIS, GENERAL COUNSEL, TRANSPORTATION TRADES DEPARTMENT, AFL–CIO

On behalf of the Transportation Trades Department, AFL–CIO (TTD) I want to thank you for the opportunity to testify this morning on the Transportation Workers Identification Credential (TWIC) and specifically on its application to port, maritime and related workers. TTD consists of 31 member unions, including those that represent thousands of longshore, maritime, rail and other workers who work in and around port facilities and who will be directly affected by the NPRM recently issued by the Transportation Security Administration (TSA) and the Coast Guard.[1] In addition, TTD directly participated in the regulatory proceeding that implemented the threat assessments and background checks for Hazmat truck drivers and continues to work with our aviation unions to address concerns that have been raised in that mode of transportation. And finally, we understand that TSA has an interest in eventually extending the TWIC program to other modes of transportation and thus our unions not directly covered by the NPRM have a vested interest in this issue. So again, thank for the opportunity to share our views and concerns.

At the outset, let me state clearly that no one wants to secure our Nation's ports and other transportation assets more than the men and women represented by our affiliated unions. Our members are on the front-lines and they will be the ones first affected in the event that a terrorist attack is carried out using or attacking our Nation's transportation system. We also understand that access control procedures, including the use of tamper-resistant identification cards, is part of this effort and

[1] Attached is a complete list of TTD affiliated unions.

we support initiatives to identify and bar individuals who pose a terrorism security risk from working in security-sensitive transportation jobs.

With that said, any TWIC program must strike the right balance—it must enhance the security of our transportation system, but must also preserve the legitimate rights of workers and not unduly infringe on the free flow of commerce. In short, the TWIC program must provide workers with basic due process rights, including a meaningful appeal and waiver process, ensure that privacy rights are respected, not force workers to pay the costs of this mandate and focus on identifying true security risks and not unjustly punishing someone twice for a bad decision made years ago.

On this point, I want to acknowledge the work of this committee in passing Section 70105 of the Maritime Transportation Security Act (MTSA) that establishes the requirements and limits for a maritime transportation security card. While not a perfect compromise, there are important protections and limitations included in this provision, and it is noteworthy that the Committee has tried to strengthen these protections since passage of the MTSA in 2002. With last week's NPRM, and the Coast Guard's earlier notice that it will check names against the terrorist watch list, the Department is in the beginning stages of implementing the TWIC maritime program required by Congress shortly after 9/11.

We are still in the process of reviewing and analyzing this voluminous proposal, and we will submit a more comprehensive response to the TSA and the Coast Guard as requested in the notice. I would like to take the opportunity this morning to highlight some of our initial concerns and reactions to the proposal and to offer some suggestions for improvement.

There is little doubt that TSA and the Coast Guard had a challenging task in drafting this NPRM and implementing the Hazmat program as required by the USA PATRIOT Act. We do appreciate the fact that in many regards the NPRM follows the mandates of Section 70105 and otherwise attempts to put forth a reasonable and workable program. Unfortunately, there are many areas, too many in our opinion, where TSA and the Coast Guard have fallen short in both fulfilling the mandates of Section 70105 and generally striking the right balance between security and fairness for workers. These two objectives are not inconsistent. To the contrary, a workable, reasonable and fair TWIC program will only enhance transportation security, and we see no reason why this proposed rule cannot be altered to better achieve this objective.

Disqualifying Offenses

We remain concerned that that the list of felony offenses that will disqualify a worker from holding a maritime TWIC is too broad, vague and not adequately focused on eliminating true security risks. Section 70105 is clear—for felony convictions, an individual may not be denied a security card unless the individual has been convicted within the past 7 years or released from incarceration in the last five, of a felony "that the Secretary believes could cause the individual to be a terrorism security risk to the United States." We maintain that some of the broad descriptions of disqualifying offenses listed in Section 49 CFR 1572.103 go beyond this mandate and this limitation.

Again, in looking at criminal records, the Secretary may only deny a card to someone who could pose a terrorism security risk. By way of example, the NPRM says that all felonies involving dishonesty, fraud or misrepresentation make an individual at least an initial terrorism security risk. If a worker is convicted of a felony in writing bad checks, that would appear to qualify as a crime of "dishonestly or fraud." While we understand why a financial institution may not want to hire that person, we simply do not understand how that makes the individual a terrorism security risk unqualified to work in a port. Simply put, there needs to be a clearer nexus between terrorism security and the crimes that will disqualify an individual from holding a maritime TWIC.

The TSA and the Coast Guard note in the NPRM that they are adopting the disqualifying offenses currently in place for the Hazmat program. While we agree that the two programs should be as similar as possible, it must be remembered that the Hazmat program and the maritime TWIC program are governed by two different statutes. Specifically, Section 1012 of the USA PATRIOT Act (codified at 49 U.S.C. 5308(a)) grants TSA broader discretion in deciding what crimes will disqualify someone from the industry and how far back the criminal record should be examined. Section 70105(c) places more limits on the Secretary for the maritime program—only those crimes that make someone a terrorism security risk to the United States should be included. In fact, during consideration of the Hazmat background check program, TTD specifically asked TSA to adopt a list of criminal offenses that in reality was consistent with the MTSA standard. While TSA claimed it was adopting

such an approach, we continue to believe that the crimes adopted for the Hazmat program and proposed for a maritime TWIC do not in fact meet the standard established by Section 70105.

In response to our calls to limit the list of disqualifying crimes, TSA has often stated that such refinements are unnecessary because a worker can always apply for waiver. While we appreciate the inclusion of a waiver process in Section 70105, and its adoption in the NPRM, it should not be used as excuse to adopt an overly broad list of felonies and allow other problems with the list of disqualifying crimes to go unaddressed.

Deeming someone a terrorism security risk is not a characterization that should be casually rendered and places an obvious burden on a person to overcome that label. While TSA may be able to report that it is granting waivers in the Hazmat program, we do not know how many workers have chosen to not apply for a Hazmat endorsement in the first place because of the long list of disqualifying offenses. Furthermore, TSA will need to review and process the criminal histories of approximately 750,000 port and related workers pursuant to this NPRM on an extremely tight deadline. On top of the other procedural challenges inherent in this program, it makes little sense to overload the waiver process with individuals who should never have been disqualified in the first place.

We are also disappointed that the proposed regulations do not provide for any mechanism for a person to challenge the determination that a particular crime is one described in Section 1572.103. There may be situations where a person is convicted of crime that TSA believes fits into the broad description of the disqualifying offenses, but a legitimate argument could be made to the contrary. To rectify this problem, we intend to ask TSA to allow workers to challenge the characterization of a particular offense either as part of the waiver or appeal process.

Waiver Process and ALJs

As indicated earlier, we worked directly with Members of Congress in the negotiations that led to Section 70105 and the inclusion of a waiver process was a major priority for our member unions. We were therefore pleased that TSA chose to incorporate this waiver into the Hazmat program and it has been offered as part of the NPRM.

However, we remain concerned that the waiver process, as envisioned in the NPRM, requires workers to apply back to the very same agency that determined the individual was a security risk in the first place. Given the high public anxiety over terrorist risks and the insular nature of this process, we are concerned that TSA might reject waivers that are otherwise meritorious.

In an attempt to address this problem, we have asked TSA, on numerous occasions, to allow workers to have their waiver cases heard, at some point in the process, before an administrative law judge (AU) at a hearing on the record. This would allow employees to make their case in front of an impartial decisionmaker not bound by political pressures or subject to agency interference. In addition, ALJ decisions would establish case precedent that would better define what constitutes a security risk. This would bring a level of fairness and consistency to a system that is central both to employee rights and national security.

Because TSA has rejected our calls for this basic protection, we have been forced to turn to Congress for redress on this point. Fortunately, this Committee has acted and an ALJ provision is included in the pending Coast Guard Reauthorization Conference Report (H.R. 889). While we understand that the Conference Report is being held up for unrelated reasons, it is clear that there is wide and bipartisan support for the introduction of ALJs into the TWIC process, and I want to thank Chairman Stevens and Co-Chairman Inouye for your help on this issue.

For reasons that are quite frankly puzzling, TSA and the Coast Guard have failed to include an ALJ in this NPRM and have simply stated they will alter the proposal if Congress changes the law. While we have every confidence that Congress will act, it is troubling that TSA and the Coast Guard are refusing to include ALJs on a technicality. These agencies clearly have the discretion to include ALJs in the process and their continued resistance to the program gives us some concern regarding how they will implement and incorporate ALJs into the TWIC process. I should note that for the ALJ process to be effective, cases must be heard and decided as expediously as possible so that employees are not unjustly barred from returning to work.

Application of Waivers to Subjective Decisions

We are also concerned that the waiver process in the NPRM does not apply to security threat assessments made by TSA for subjective reasons under Section 1572.107. Under this Section, TSA can disqualify someone for criminal offenses that

are not on the disqualifying list, if the TSA determines that other convictions are "extensive," if the conviction is for a "serious" crime, or if the person was imprisoned for over 1 year. Putting aside our concerns with these broad and subjective criteria, we do not understand how TSA is implementing this without allowing workers to seek waivers as they do for crimes listed in Section 1572.103.

More to the point, Section 70105(c)(2) of the MTSA specifically mandates that TSA afford a waiver for all reasons a worker may be disqualified from holding a transportation security card. We understand that TSA does not afford waivers under the Hazmat program for disqualifications for subjective decisions. While we objected to that decision in the Hazmat proceeding on policy grounds, the case here is different—for the maritime TWIC, a waiver is a statutory right and cannot be denied by TSA at is discretion. We hope and expect TSA to make this change as it finalizes its rule.

National Standard Needed

We are concerned with language in the NPRM that would specifically allow states to impose additional and broader background checks and to do so without any of the protections or limitations included in the Federal program. If security threat assessments are needed to enhance our national security, the TSA should adopt and enforce a national standard. It makes little sense for TSA to establish a national program, force workers to pay for this program (over our objections), and then allow local jurisdictions to use national security as an excuse to create yet another security review process.

There simply should not be a difference in what constitutes a security risk based on what state or jurisdiction a port resides in. Furthermore, TSA and the Coast Guard have a stated intent, both articulated in the NPRM and in other documents, to achieve a level of consistency governing threat assessments and transportation credentials. Allowing states to arbitrarily impose different security requirements is inconsistent with this objective and should be reversed. Failing that step, TSA must ensure that due process and privacy rights provided for at the Federal level apply to the states. We would note that Congress specifically mandated this for the Hazmat program in the SAFETEA–LU legislation and we would expect TSA to extend this to the maritime side. We will also seek clarification from TSA on how it intends to evaluate and enforce the requirement that states, with separate checks, comply with these statutory due process requirements.

Cost of the TWIC

We are vehemently opposed to the provisions of the NPRM that passes one hundred percent of the costs of this program on to individual workers. The security threat assessments and the background checks mandated in this proposal are considered necessary to enhance the security of our Nation's ports and are part of the overall effort to fight terrorist elements. Given the reality of this national priority, the government, and not individual workers, must absorb the costs of this program.

We understand that the DHS Appropriations Act (Pub. L. 108–90, Section 520) directs TSA to "charge reasonable fees for providing credentialing and background investigations in the field of transportation." We would respectfully ask that Congress lift this appropriations rider and allow the Federal Government to fund this program in a reasonable manner. We would note that even with the rider in place, nothing requires the costs be absorbed by workers—it simply states that "reasonable fees" be charged. The TWIC card, and the accompanying background check, is essentially a condition of employment and will surely benefit our employers. The port and related facilities will be more secure and access control procedures will be in place through readers and biometric cards. If the Federal Government refuses to step in and fund this security mandate, employers must be required to fund a program that will directly benefit their operations. It should be remembered that employees will have to go through the time and effort to apply for this card and may incur additional expenses if an appeal and waiver are needed. It is neither fair nor reasonable to ask them to also pay for a security mandate that has broader benefits.

Transportation Security Incident

Under Section 70105(c)(1)(A)(ii) of the MTSA, an individual will be denied a maritime TWIC if he has committed a felony, within the last 7 years, that causes "a severe transportation security incident." The MTSA further defines this term to include a security incident that results in a "transportation service disruption" or an "economic disruption in a particular area." In both the Hazmat rule and in the maritime TWIC NPRM, TSA has made a "transportation security incident" a permanent disqualifying offense with no waiver opportunities. We have long been concerned with the broad definition of this offense and that it could be interpreted to include a wide range of activities that while disruptive to commerce or transportation,

should not permanently disqualify a person from holding a TWIC. We are pleased that Congress, again in the SAFETEA–LU legislation, included a provision that attempts to limit the reach of this provision and TSA has modified its rules accordingly. Nonetheless, we remain concerned that the term could still be misused, and we will urge further clarifications as the process moves forward.

Privacy of Information

As we have consistently stated, maintaining the privacy and confidentiality of the information collected and generated by the TWIC process is crucial. Toward this end and at our request, Section 70105(e) includes a specific mandate that "information obtained by the Attorney General or the Secretary under this section may not be made available to the public, including the individual's employer." Consistent with this requirement, information that is gathered from the use of the card, *i.e.,* when the employee enters and leaves a port facility, must not be shared with the employer. The TWIC program was conceived and mandated by Congress to enhance the security of our Nation's seaports. For this effort to succeed, it must remain solely focused on that objective and not be used for any non-security reason. We will continue to work with TSA and the Coast Guard to ensure that this issue is addressed in the final rule.

Application of TWIC to Aviation

As the Committee is well aware, Congress has mandated that workers in the aviation sector undergo separate threat assessments, including a review of criminal histories. I should note that aviation workers are still denied access to a waiver process, rights afforded to Hazmat and maritime employees, and this double-standard should be rectified. Even though these threat assessments are in place, electronic identity cards have yet to be issued by TSA. Given the unique nature of the aviation industry, and the mobility of its workforce, an electronic biometric identification card would allow these employees to move more efficiently through the system and at the same time enhance aviation security. I know the Air Line Pilots Association (ALPA) has a particular interest in pursuing this issue and has specifically offered its assistance to Secretary Chertoff in this regard. We hope that TSA will work with our aviation unions to implement an aviation TWIC card based on the checks that have already been completed on those employees and consistent with the protections and limitations previously articulated.

Customs Problem

Before I close, I want to raise a specific problem for workers who must work in Customs-controlled areas. These workers are subject to separate background checks that give individual port directors great leeway in making these threat assessment decisions. In particular, a port director can use a felony conviction to disqualify someone even if that felony was committed well beyond the seven or 10 year look-back period that govern maritime or aviation respectively. In fact, there have been several situations where an airport worker, after passing an extensive background check required by the aviation statute, had his or her customs credentials pulled because of a felony conviction older than 10 years. This double-standard makes no sense and has no security-based rationale. As TSA moves forward with efforts to avoid duplication of background checks, this problem and similar issues must be resolved.

Final Thoughts

As stated in the outset, transportation labor has always supported policies that will enhance the security of the Nation's seaports and our entire transportation system. We understand and recognize that the TWIC program is part of the Federal response to terror, and we specifically support its stated purpose of preventing terrorist elements from infiltrating our transportation network. But for this program to be successful, the legitimate rights of workers must be preserved and those that pose no terrorist threat must not be denied their right to work in this industry. We look forward to working with this Committee, the TSA and the Coast Guard to meet this objective and to make improvement to this proposal.

Thank you again for the opportunity to share the views of transportation workers.

ATTACHMENT—TTD MEMBER UNIONS

The following labor organizations are members of and represented by the TTD:

Air Line Pilots Association (ALPA)

Amalgamated Transit Union (ATU)

American Federation of State, County and Municipal Employees (AFSCME)

American Federation of Teachers (AFT)
Association of Flight Attendants—CWA (AFA–CWA)
American Train Dispatchers Association (ATDA)
Brotherhood of Railroad Signalmen (BRS)
Communications Workers of America (CWA)
International Association of Fire Fighters (IAFF)
International Association of Machinists and Aerospace Workers (IAM)
International Brotherhood of Boilermakers, Blacksmiths, Forgers and Helpers (IBB)
International Brotherhood of Electrical Workers (IBEW)
International Federation of Professional and Technical Engineers (IFPTE)
International Longshoremen's Association (ILA)
International Longshore and Warehouse Union (ILWU)
International Organization of Masters, Mates & Pilots, ILA (MM&P)
International Union of Operating Engineers (IUOE)
Laborers' International Union of North America (LIUNA)
Marine Engineers' Beneficial Association (MEBA)
National Air Traffic Controllers Association (NATCA)
National Association of Letter Carriers (NALC)
National Conference of Firemen and Oilers, SEIU (NCFO, SEIU)
National Federation of Public and Private Employees (NFOPAPE)
Office and Professional Employees International Union (OPEIU)
Professional Airways Systems Specialists (PASS)
Sheet Metal Workers International Association (SMWIA)
Transportation Communications International Union (TCU)
Transport Workers Union of America (TWU)
United Mine Workers of America (UMWA)
United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW)
United Transportation Union (UTU)

The CHAIRMAN. Well, thank you very much for that.

Let me call on our Co-Chairman first this time.

Senator Inouye?

Senator INOUYE. Mr. Willis, your position is that if the conference bill is adopted with the administrative law judges involvement, that would meet your requirement of due process?

Mr. WILLIS. Yes. I think for the purposes of the waiver process, the administrative law judge is a critical component for due process, and that is a provision that, obviously, we have supported, and we think is a good provision. I will say, though, as I said in my opening statement, that part of due process is coming up with a list of disqualifying offenses that is not too broad and too vague. Simply because you have a good waiver process and a good ALJ process, it doesn't change the fact that you have to narrow those crimes. And I think it's also important to note that once you have an administrative law judge, those cases need to be heard quickly and efficiently, because you're going to be keeping that individual worker out of a job, I believe, under the TSA rule. So, that is an important component of the due process question.

Senator INOUYE. Are you, at this moment, discussing this matter with TSA?

Mr. WILLIS. We have clearly raised the need for an ALJ provision, both in the context of the Hazmat proceeding and—before the rule came out on this topic. Quite frankly, we were a little puzzled

that they didn't just go ahead and include the ALJ in the NPRM, stating that if Congress were to change the law, then they'll do it in their final rule. Given that you're so close on that, and given that there is wide bipartisan support for an administrative law judge, we would have preferred to see TSA just do it. They clearly have the discretion to include it. So, that's something that we're going to continue to work on, both legislatively and in the regulatory proceeding.

Senator INOUYE. Thank you very much.

Mr. Cummings, you noted in your testimony that the cost associated with the program must be not only reasonable for individuals, but also for facilities and vessels.

Mr. CUMMINGS. Yes, sir.

Senator INOUYE. Now, we have been advised that the total cost for the nationwide implementation of TWIC is going to cost between $1.1 billion to 1.9 billion. And the cost for facility owners will be estimated between $580 million and $1.2 billion. Do you think this is reasonable? Or how is this cost going to apply to the 50 facilities in your area, Los Angeles/Long Beach?

Mr. CUMMINGS. Yes, sir. In our port, both Los Angeles and Long Beach are landlord ports, so the individual terminals have to comply with these regulations, and that relationship is between them and the United States Coast Guard. So, as was published in the notice of proposed rulemaking, if it follows along those lines, these individual terminals will then have to fund the installation of the systems on their own terminals—the card-reading systems—so that their terminals will be in compliance with the Coast Guard regulations.

Senator INOUYE. What will be the cost implication for your area for the 50 facilities?

Mr. CUMMINGS. On a—it's hard to say, exactly, Senator. On a—the way the notice of proposed rulemaking is set up, the requirement is for one individual reader to be installed to meet the requirements. I think our experience is that on many of our terminals, particularly the larger ones, they will require significantly more system installation than just a single reader. Estimates we've made, on a per-terminal basis, is more on the order of $200,000 or so. I think that's considerably higher than an estimate that's just based on a single reader. So, there will be discretion at—on the part of the terminals, in terms of how widely and what investment they make. And they'll make those decisions based on their operations and their need for expediency and flow, and also, again, to meet the Coast Guard regulations.

So, we expect that it'll be more along the lines of more cost to the terminals than was estimated in the rulemaking, more on the order of $100,000 to $200,000 per terminal, at least the larger terminals, Senator.

Senator INOUYE. Do you that will be reasonable?

Mr. CUMMINGS. I think, for our terminals, they have—they have all demonstrated strong commitment. As I mentioned in my testimony, all of our terminals, as soon as the initial Coast Guard regulations came out, they were all very expedient in getting their plans done and submitted. They made the monetary investments that they needed to make on their terminals. I'm confident that all

of our facilities will follow suit and make whatever investments they need to make to continue to comply with the full implementation of the program.

Senator INOUYE. In implementing your program, will these facilities have to be examined by you, and approved?

Mr. CUMMINGS. No, sir. The approval process will be by the United States Coast Guard. We will function as a port authority in our capacity. We'll function as a facilitation entity between the terminals and the Coast Guard. We'll do what we can to promote both the system installation process, as well as the credentialing process, for our—we consider our stakeholders our—you know, our longshore populations, the truckers, as well as the terminal employees, so we will—we'll work as—any way we can to accommodate and facilitate the process.

Senator INOUYE. You'll have to receive the approval of the Coast Guard.

Mr. CUMMINGS. The terminals—yes, the terminals will, in the end, require an approval of a plan—a plan amendment and then the actual installations to support the TWIC program.

Senator INOUYE. Ms. Himber, the same question. Do you have a lot of port facilities there?

Ms. HIMBER. We have roughly 40 facilities along the three states on the Delaware River. And I have not had the opportunity, since the proposed draft regulation came out last weekend, to go through, with my members, how they feel that the costs will affect them, and whether or not they think it's reasonable.

A few things that I did notice in the proposed rulemaking that were not included, in addition to only costing out potentially one reader site at each facility—which does not seem to be reasonable; it's quite likely that all of the facilities will require more than one—there was also no consideration taken to the software costs which might be required to integrate the TWIC readers with the facilities' internal access control software and system. So, whether or not the estimate that—it does strike me that the estimate that TSA's put together may be a little bit low.

Senator INOUYE. I thank you very much.

Thank you.

The CHAIRMAN. Thank you, my friend.

First, let me say, Mr. Cummings, I appreciated the courtesy that your people showed me and my staff when we did visit the Los Angeles Port.

Mr. CUMMINGS. Thank you, Mr. Chairman.

The CHAIRMAN. Having gone to high school in that area of the South Bay, I can tell you it's changed considerably since the last century.

Mr. CUMMINGS. Yes.

[Laughter.]

The CHAIRMAN. You seem to have an access problem that goes beyond just identification. I note there's only one railroad line going in and out. Have you covered the question of the contents of the containers that come and go into the port? Are you working on that security, also?

Mr. CUMMINGS. Yes, Mr. Chairman. We're working on a number of different ways on cargo security. We are participating in Oper-

ation Safe Commerce, which is entering its third phase, and that program, as you may know, is intended to identify and test leading-edge and effective and efficient cargo security measures that then can be implemented industry-wide. We continue to work on—with our terminals and with the U.S. Customs and Border Protection, both at the national level and within the port, to implement their programs, such as the Radiation Portal Monitor Program, which is the radiation detection screening at the out-gates of the terminals. And for our port, that is—that installation is nearly complete. I believe they're just about finished with those installations.

The CHAIRMAN. When I was there, I felt there was a question as to whether the same identification should be required of people who drive these containers to the port as will be required for those people who work in the port. Are you going to have two sets of identifications?

Mr. CUMMINGS. No, Mr. Chairman. The way that the TWIC program is laid out, and the way we've understood it in—during our participation in its development is that it would just be this single credential that would apply to anyone who requires the unescorted access on the maritime terminal that's—as dictated in the regulations. So, to our way of thinking, that actually will work fine. The single definition and the single card would be suitable.

The CHAIRMAN. Well, Mr. Willis, a person who is driving a truck that has got containers on it does not necessarily have a Hazmat identification, does he?

Mr. WILLIS. That container may or may not include Hazmat. Regardless, they—if they're going to have regular access, they are still going to be, under this NPRM, required to have a TWIC, as are the rail workers that we represent.

The CHAIRMAN. You're saying all the people who are involved in the trucks that come and go, and all the people involved in the trains, operating the trains and the cars that come and go into the port, they will have the TWIC. Is that the plan?

Mr. WILLIS. If they need regular unescorted access to a secure area of a port, yes, they will need a TWIC, under this NPRM.

The CHAIRMAN. Well, now, that brings me back to you, Mr. Cummings.

Mr. CUMMINGS. Yes.

The CHAIRMAN. There is a secure area beyond which everybody has to have it. What percentage of the port is actually a secure area?

Mr. CUMMINGS. Mr. Chairman, in our port, as you're familiar with from your visit, it's the—the port complex overall is fairly broad, encompassing the two port authorities and the two cities. Within it are these 50 individual terminals. For our port, that's where the security begins. It's at the gate of each of those individual facilities. And, for the most part, they have deemed that the entry into their area restricted, because they consider everything within their gates their responsibility to maintain security over—the highlines, the cargo transition points, all the buildings and so forth. So, they are, for the large—for the vast majority, just maintaining the one single perimeter. So, that will be the point at which unescorted access within that area will require the TWIC card.

The CHAIRMAN. So, you're not going to have a single entry into that big port, are you?

Mr. CUMMINGS. No, sir. We'll just maintain the current structure with the 50 individual terminals.

The CHAIRMAN. But if a person has a card and wants to go to any one of those terminals, that same card will let them get into any terminal, right?

Mr. CUMMINGS. Only—according to the regulation, only if that individual facility has listed that person on their system. In other words, each of these 50 terminals will then have the authority to only grant this unescorted access to those TWIC cardholders. So, the first step, Mr. Chairman, would be to get a TWIC card. The second step would be to present yourself at a facility and convince them that you need unescorted access on their terminal. They will—they'll enter you into their system, their database, and you will then proceed.

The CHAIRMAN. That means that every one of those terminals has to have a card reader?

Mr. CUMMINGS. Absolutely. Yes, sir. Multiple, probably, in most cases.

The CHAIRMAN. You've got the same problem, Ms. Himber?

Ms. HIMBER. Yes. Most of the facilities in the Delaware River have designated the entire perimeter as the—anything inside the external perimeter as a secure area.

The CHAIRMAN. Well, as I recall getting into the Port of Los Angeles, it's going to be a redundant thing. You're going to have a couple of places where you have to be identified, right?

Ms. HIMBER. Right. And you might have multiple truck lanes at the main gate, so each one of those lanes, potentially, would have to have a reader, plus a visitor lane.

The CHAIRMAN. Mr. Willis, in terms of what your people are doing, as I understand it, you question the financial impact on the individual, right?

Mr. WILLIS. That's correct.

The CHAIRMAN. Who's going to be required to make sure the persons that are operating these vehicles have cards, the owner of the trucks or the individual member?

Mr. WILLIS. Well, I think how it's going to work is that if you come up to a port, you're not going to be able to have unescorted access unless you have a TWIC. I think with the truck drivers, it's going to be a complicated issue, because many of these—most of these, I believe, are independent contractors. I think that with the folks that work regularly in the ports and those who work in the rail, obviously they have a consistent employer, so there's going to be some connection there, and some ability to communicate with those workers and make sure that they are applying for the TWIC in a timely manner, and some infrastructure there.

The CHAIRMAN. Are there any other identifications that are required of your members that—to be involved in this activity?

Mr. WILLIS. Well, I mean, clearly there are a whole set of documents, as you mentioned, that the mariners need and that the Coast Guard is trying to figure out how you merge those. And that's going to be something that we're very interested in.

The CHAIRMAN. But they have to have their own driver's license, right?

Mr. WILLIS. Our members, you mean? Or the mariners?

The CHAIRMAN. Yes, your members.

Mr. WILLIS. Well, for the truck drivers to get a CDL, obviously you need a driver's license. And for the port workers, the TWIC would be the main identification.

The CHAIRMAN. Well, currently isn't there an identification card they have?

Mr. WILLIS. Sure. For individual ports—I can't speak for all of them, but, some ports are going to have—may already have current identification cards.

The CHAIRMAN. Do you have them, Mr. Cummings?

Mr. CUMMINGS. We do not have a port identification card, no, sir. The access to our terminals right now is based on a driver's license or, for our longshoremen, their union card.

The CHAIRMAN. How about you, Ms. Himber?

Ms. HIMBER. Some ports in the Delaware region have issued port site-specific cards, and others are using a driver's license.

The CHAIRMAN. And who pays for them now?

Ms. HIMBER. The individual facility.

The CHAIRMAN. I've got some questions I'd like to submit to you, too. We've got to go to the floor to have a vote.

I appreciate very much your help. We'd like to be able to work to find a way to reduce the cost of these cards. And maybe you're right, by the time we get the quantity-based concept, the cost will go down.

Have any of you thought about the idea of having private companies do this? Have you, Ms. Himber?

Ms. HIMBER. We've thought about it. In fact, we even talked about it, at one point during the course of the pilot program, about 2 years ago, and we met with TSA and other—from Florida all the way up to New York on the East Coast, and looked at other opportunities to do this. But, at that time, we were told by TSA that they were nearing completion of whatever the current phase was, so we discontinued those discussions in favor of the TWIC.

Mr. WILLIS. I would only add that if you're going to have—and clearly I think this is where TSA is going—if you're going to have a private contractor issue these cards and participate in this program, there are significant requirements, both in statute and regulation, as far as protecting the privacy of the worker, making sure that the information is only used for security purposes, and isn't disclosed to employers or the public, and that these cards have to be, you know, given out in a quick fashion and quick turnaround time, so that any private entity that does provide these services—you really have to look to make sure that they're prepared to do that and that there is a process where that can be assured.

The CHAIRMAN. Well, that's true. But they're going to contract that out, anyway.

Mr. WILLIS. Exactly. I think as they look at that——

The CHAIRMAN. As a practical matter, it's going to be in some private sector. I just don't know why the whole thing wasn't looked at as being a private-sector objective—something that'll be nationwide, that it would bring the cost down considerably.

Senator Inouye, do you have any further questions?

Senator INOUYE. No, thank you.

The CHAIRMAN. We want to work with you to make sure this system works, our bill would set a drop-dead date. Do any of you disagree with that?

Ms. HIMBER. No.

Mr. CUMMINGS. No, sir.

The CHAIRMAN. Mr. Willis?

Mr. WILLIS. No.

The CHAIRMAN. Thank you very much. We appreciate your coming.

[Whereupon, at 11:50 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF AMERICAN TRUCKING ASSOCIATIONS, INC. (ATA)

American Trucking Associations, Inc. (ATA) appreciates the opportunity to submit comments on the Transportation Worker Identification Credential (TWIC). ATA is a federation of motor carriers, state trucking associations, and national trucking conferences created to promote and protect the interests of the trucking industry. ATA's membership includes more than 2,000 trucking companies and industry suppliers of equipment and services. Directly and through its affiliated organizations, ATA encompasses over 34,000 companies and every type and class of motor carrier operation. The trucking industry is the one mode of transportation that connects all other modes of the supply chain. ATA's motor carrier members are, on a daily basis, transporting containers in and out of our Nation's seaports, rail terminals, and airports. The screening of individuals involved in the transportation of goods is important to the trucking industry.

Any discussion of the TWIC should start with the underlying concept of the TWIC and why it was deemed necessary. In January 2003, Admiral Loy, then the second most senior official at the Transportation Security Administration (TSA), summed it up best, stating:

> A fourth initiative also underway is development of a Transportation Worker Identification Credential or TWIC . . . The idea is to have these [transportation] employees undergo only one standard criminal background investigation . . . I've heard that there are some truck drivers currently carrying up to 23 ID cards around their necks. I wouldn't want to pay that chiropractor bill. Under the TWIC program drivers and other transportation workers will only have one card to deal with which would be acceptable across the United States.—Remarks of Admiral James M. Loy, Under Secretary of Transportation for Security, Transportation Security Administration, before the Transportation Research Board 82nd Annual Meeting Chairman's Luncheon, January 15, 2003.

As the representatives of the trucking industry, ATA supported this concept of a single background assessment and the issuance of a single security credential. However, since Admiral Loy's speech in January 2003, the trucking industry has witnessed the implementation of a background check process for individuals obtaining hazmat endorsements (HME), a different background check requirement for truckers going to secure areas of airports, and now the implementation of yet another background check process for truckers transporting cargo in and out of the seaports. To obtain these different credentials, applicants must appear at different enrollment facilities, adapt to different administrative procedures, and pay steep "user fees" for each process required. The chiropractor bill is not the only hefty bill the trucker is paying. The bad news is that TSA has not been faithful to its vision of the TWIC. The good news is that it is not too late to get it right.

ATA urges this Committee and TSA to return the TWIC to its initial moorings. We believe the following principles will facilitate achieving the original, laudable goal: (1) the current multitude of federally-mandated background checks should be consolidated into one check that evidences an individual's privileges, from a security standpoint, to access areas or goods in the transportation supply chain; (2) the TWIC should serve not only as the one background check but also the one credential for access from a security perspective—this means the states should not be allowed, without demonstrating some compelling need, to add additional security checks and/or credentials; and (3) the system should be designed so that costs are minimized and evenly spread over all users. Adhering to these principles, a system can be implemented which truly will enhance the security of our country, while minimizing the cost of discovering the few bad apples in the large barrel of patriotic individuals who make their livings on our Nation's highways.

In developing the HME background check, TSA intended to harmonize the HME check with the check required under the Maritime Transportation Security Act of

2002 (MTSA), the law authorizing use of TWIC in the seaports.[1] Under the HME check, a driver submits fingerprints and biographical information and is checked against multiple criminal history, intelligence, terrorist, and immigration databases. Under the proposed TWIC rule, an individual requiring unescorted access to secure areas of the seaport (*e.g.,* a truck driver) would submit fingerprints and biographical information and be checked against the same databases. Furthermore, the disqualifying criteria for TWIC are the same as the criteria for HME. Although these portions seem to have been harmonized, they were not consolidated. An individual who has successfully cleared the HME background check still has to undergo a costly "enrollment" process for issuance of the TWIC (while the individual saves some money on the threat assessment portion, the cost is still expected to be $105).[2] Conversely, ATA can think of no reason why an individual who cleared the TWIC background check should not be deemed to have met the HME background check. That individual should not have to undergo any additional process from a security perspective.[3]

Other security programs that include background checks on truck drivers, such as the secure identification display area (SIDA) at the airports or the Department of Defense's clearance to haul arms, ammunition or explosives, have not been consolidated at all. The individual would have to undergo a separate check for each program. To the extent possible, ATA supports harmonizing these programs and the disqualifying criteria for these programs. ATA understands that some programs may have more stringent criteria than others, and thus a tiered level of clearance may be necessary. Nevertheless, this could still be established through one background check. TSA's proposed definition of a TWIC as a federally-issued biometric card issued to an individual who has successfully completed a security threat assessment suggests that one check for multiple programs should be sufficient.

ATA continues to share Admiral Loy's concern for the well-being of truck drivers weighed down by a multiplicity of cards. The proposed TWIC rule, by allowing state authorities to impose additional requirements for access to the ports, is an invitation for each port authority to issue its own credential on top of the TWIC. The State of Florida is already doing so at its seaports. The regulations issued by the Coast Guard under MTSA properly claimed the need for national standards of security and claimed preemption. ATA supported this eminently sensible position. ATA is disappointed that TSA has not adopted a similar approach, as the need for national standards of security remains equally applicable.

One rationale frequently proffered by states that require additional checks of their state criminal history databases is that their state databases are more comprehensive or fully populated. The failure of states to upload criminal history information to the FBI's national databases actually creates a security loophole rather than bolstering security. For example, an individual may commit a disqualifying offense in Florida that is only in the Florida database but has not been uploaded into the FBI's database. That individual would not be able to get a TWIC at one of the Florida ports but he/she could get the TWIC from a South Carolina port, because the check against the FBI's database will not reveal the disqualifying offense in Florida. If the disqualifying offense indicates that the individual is a threat in Florida (which purportedly is the rationale for having a list of disqualifying offenses), then that same individual is also a threat in South Carolina. The failure to upload state data in a timely manner is a problem that needs to be addressed for the security of the whole.

Other than the differences between the criminal history databases, it is difficult to conceive of scenarios where a state's judgment on security of the Nation's supply chain should supplant the Federal Government's considered judgment. If such a scenario exists, however, the state should have to make the case to Federal authorities on a case-by-case basis. Otherwise, the Federal standards should be controlling. This, and the consolidation discussed earlier, would help return the TWIC to being the "one card to deal with which would be acceptable across the United States."

Finally, ATA understands that securing the Nation's supply chain involves costs. The trucking industry is willing to bear the cost of one—but not multiple—back-

---

[1] "[T]he agency plans to harmonize, to the extent possible, all of the various background checks that are required by statute, and so elements of MTSA appear in this rule." 68 Fed. Reg. 23852, 23853 (2003); "TSA intends to maintain as much consistency as possible between the current hazmat driver and future maritime programs." 69 Fed. Reg. 68720, 68726.

[2] The proposed rule provides for the costs to these individuals for enrollment to range from $95–$115; however, TSA has specified the $105 amount in several presentations, including a summary of highlights of the proposed rule.

[3] ATA agrees that the individual should still have to meet all the knowledge, skills and safety requirements for issuance of the HME.

ground checks and security credentials. The stovepipe approach to security programs taken by TSA has resulted in the unnecessary imposition of wasteful costs.

As discussed above, the processes for submission of fingerprint and biographical data for the HME background check and the TWIC background check are essentially the same. The main difference is that, under TWIC, the individual has a photograph taken and ultimately receives a security credential. A driver that has undergone the HME background check process pays a fee of $94 in 34 states (including D.C.) that use the TSA contractor for information collection. This fee included paying for nearly $4.8 million to set up the TSA Screening Gateway. Under the proposed TWIC rule and TSA briefings on the rule, that same driver will be asked to pay another $105 for the TWIC process. While the cost justification in the proposed TWIC rule is sufficiently vague to prevent us from knowing what the categories of costs are covering, ATA finds it hard to believe that the cost for taking a digital photo and producing a biometric card amounts to $105—particularly when a cost estimate from another government agency for the production of similar biometric cards is in the $10–$12 range. In justifying this $105 cost, TSA has stated that $45–$65 is for information collection, *i.e.,* the same fingerprints and biographical information already submitted for the HME process plus a digital photograph.

Since the HME background check rule was promulgated after passage of the MTSA requirement, it seems that reasonable forethought would have suggested storing the fingerprints and biographical information of HME driver-applicants. This would have meant the only information collection cost would have been the capture of a digital photograph. Surely, that would not cost between $45 and $65. However, TSA chose a non-uniform approach to information collection, allowing states to elect to conduct the information themselves or use a TSA contractor. In the 17 states electing to conduct information collection themselves, TSA has no control over what happens to the fingerprints. ATA hopes that TSA will address these types of self-erected hurdles that simply add to the costs borne by the trucking industry.

The consideration of the TWIC concept transportation-wide began as early as December 2001. Its implementation has been marred by numerous delays. Admittedly, there are a number of issues to consider and get right. ATA is alarmed that, rather than building a scalable program that is true to the concept laid out by Admiral Loy and his predecessors, TSA is simply building another stovepipe program to screen workers at the seaports.

ATA does not oppose background checks of individuals in the trucking industry. ATA *does* oppose the wasteful expenditure of resources—both government and private sector—that comes with conducting multiple background checks of the same individual against the same databases. The trucking industry has consistently demonstrated its willingness to contribute to the security of the homeland and its willingness to pay the costs related to driver screening. In return, ATA simply asks that these costs be reasonable and part of an efficient process. ATA supports an approach that is good for security—and good for commerce.

JOINT PREPARED STATEMENT OF JAMES KNEELAND, DIRECTOR, PROJECT MANAGEMENT OFFICE, FLORIDA DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES; AND FLORIDA HIGHWAY PATROL COLONEL BILLY DICKSON (RETIRED), FLORIDA UPAC TSA LIAISON

Florida Perspective—Introduction

First of all, Florida firmly believes that the Transportation Workers Identification Credential (TWIC) has the potential to be the archetype of a secure credential.

During the past 2 years Florida has worked closely with TSA and believes that the implementation of a Transportation Workers Identification Credential is a key ingredient to national security at transportation modes.

This document is not meant to be a criticism of any entity or person but instead will hopefully provide some additional insight into a methodology for implementation.

We have identified a chronology of events culminating with recommendations. In addition, we have learned several valuable lessons which we would like to share with the Committee.

I. Detailed Events Timeline

2003

- June—Florida passes Section 311.125, Florida Statutes, mandating a biometric credential for Florida's public entity seaports modeled on the TWIC standard.

- (July to October)—Florida builds team and requirements document for a Florida Uniform Port Access Credential (FUPAC).
- (October–December)—Florida negotiates with TSA for a Memorandum of Understanding (MOU) and Memorandum of Agreement (MOA).

2004

- January—Florida signs a MOU with TSA.
- February—Florida signs MOA with TSA.
- February to June—Florida assists with TWIC design.
- June to August—Florida participates as a member of Request For Proposal Committee to evaluate technology vendors.
- August—TSA Awards prototype contract (Phase III) to BearingPoint.
- September—HSMV was advised by TSA that the Phase III Prototype would involve an Initial Operating Capability (IOC) which was basically a prototype of a prototype.
- November—End of November finish IOC.
- December—Florida meets with vendor (BearingPoint) and then reports to TSA that the system has potential problems.

2005

- January—Florida meets with TSA in Washington, D.C., to identify the potential problems and highlights a number of significant issues with the system.
- February—Concerned about the system Florida meets with TSA who reaffirm support.
- March—Florida meets with TSA—still problems with system, TSA assures Florida system will be ready in April.
- April—Florida outlines several concerns to TSA via e-mail.
- May—TSA claims system is ready. Florida advises TSA that a User Acceptance Test must be performed before rollout to Florida seaports. TSA reported they could not test because printing capability was not activated at the Federal Card Production Center.
- June—Florida checks TSA enrollment centers and discovers significant issues with the enrollment process.
- June—End of June TSA reports they are shutting program down due to budgetary constraints.
- July—Florida Governor's office intervenes (Office of Drug Control) and TSA meets with the Governors office. TSA agrees to review the feasibility of sustainment for Florida.
- August—TSA meets with Florida program directors and acknowledged that the system does not work properly so program would close down but proffers to print cards for Florida at $10 per card in Corbin, Kentucky.
- September—Following several discussions, TSA and Florida agree to perform a User Acceptance Test (UAT) to verify system works properly.
- October and November—UAT is conducted. System still has problems but Florida agrees to move forward at meeting in Governor's office with TSA, provided that TSA would appropriately support the system.
- December—Florida team meets in Washington, D.C. with TSA. TSA promises support so Florida sets up Pensacola to be first port scheduled for activation on January 9, 2006.
- December 29—TSA notifies Florida that, due to lack of funds, they are delaying the program until further notice.

2006

- February—Lacking response from TSA, Florida moves forward with Risk Mitigation plans.
- February 21—TSA informs Florida that they can retain use of the enrollment centers, however, cannot use the biometric/ICC cards (60,000).
- February, March, April—Florida begins implementation of its Risk Mitigation Plan (FUPAC Implementation.)
- April—TSA notifies Florida of TWIC badge revocations. Florida queries TSA and is told that the entire system has been taken down.

II. History

1. The 2003 Session of the Florida Legislature passed and Governor Bush signed into law an amendment to Chapter 311, Florida Statutes, adding § 311.125, Florida Statutes. The amendment mandates a Florida Uniform Port Access Credentialing (FUPAC) system and charged the Department of Highway Safety and Motor Vehicles (DHSMV) with design, implementation and management of the new credentialing and access control system. Prior to the passage of the legislation, commercial interests who engaged in business on multiple Florida seaports were required to obtain and pay for access credentials, including multiple fingerprint-based background checks for each port.

2. The 2003 legislation strengthens security by creating a central credential repository in the Florida Department of Highway Safety and Motor Vehicles (DHSMV), adding modern security elements to the credential, alleviating the concern of stakeholders related to the cost of multiple credentials [1] for the public port system in Florida.

3. While the statutory revision charged DHSMV with the development of the credentialing and access control system, the revised statute also called for DHSMV to act in consultation with the Florida Department of Law Enforcement; Florida Seaport Transportation and Economic Development Council; Florida Trucking Association; modeling on the TSA TWIC in the development of a Uniform Port Access Credential System that provides a biometric confirmation of claimed identity and on-site verification of access authority for all persons having business necessity aboard a public seaport. The statute retains the granting of access privileges to the seaport and continues the authority of seaports to allow access to seaports for visitors and persons having limited business necessity without a permanent port access credential.

4. As noted above, a key component of the statutory revisions called for the FUPAC to be modeled on the emerging Transportation Workers Identification Credential (TWIC) under development by the Transportation Security Administration (TSA).

5. In 2003, a $3 million Federal grant was awarded through the Office of Domestic Preparedness (ODP) to DHSMV for the design, development and implementation of the TWIC/FUPAC project.

   a. The majority of the grant was allocated to the development and implementation of the state access control system and its interface with the TWIC card.

6. At the request of TSA, Florida provided a Florida Integrated Project Team leader (FIPT) who was embedded with TSA for 6 weeks in Washington D.C. for training and development of a long-term MOA between TSA and DHSMV. DHSMV selected a team leader with over forty years of experience in law enforcement, credentialing and criminal investigations related to credentialing fraud. The Florida IPT, Col. Billy Dickson, is considered to be a national expert on identity issues, regularly serving on national committees for AAMVA, the American Association of Motor Vehicle Administrators.

7. In early 2004, TSA replaced the Florida IPT with a Federal FTE position and removed the DHSMV position. However, Florida retained Col. Dickson. Well-known and respected throughout Florida and the country, Col. Dickson continues to serve as liaison with TSA and act as an advocate for the Florida seaports, as well as coordinating the implementation effort.

8. In 2004, Florida also hired an Information Technology (IT) expert to serve as Director of the program for Florida. The Director, James Kneeland, has over 30 years experience as a CIO and IT Architect. He has successfully installed dozens of systems and has experience as a Systems Engineer with EDS, and helped implement the National Flood Insurance program in 1978 and a Medicare-A system that became a HCFA standard in 1985. As a Senior Executive and CIO with the Massachusetts Registry of Motor Vehicles, he also implemented the first imaged licensing system in the United States. He has taught IT for 22 years at Northeastern University and is a certified PMP (Project Management Professional). A nationally recognized expert in IT, Project Management and Credentialing, the project Director was viewed as the ideal selection to balance a complex IT credentialing project.

9. A Memorandum of Agreement (MOA) between TSA and DHSMV was signed in February 2004. In essence, it's a requirements document indicating the responsibilities of TSA and the responsibilities of DHSMV. The MOA codified a Federal/

[1] Truck drivers were required to purchase a separate credential at each port requiring a separate background check at each port. The new statute provided for a single Florida credential and one background check valid at all ports.

state partnership to enhance the security of Florida's public seaports. The MOA assigned responsibility to TSA to design, develop and implement a Federal credentialing system that includes applicant vetting, threat analysis and ties claimed identity to an individual through the Federal I–9 form.[2] Claimed identity would be verified and tied to the individual through a reference biometric (fingerprint) that would be retained in the Federal Identity Management System (IDMS) and would be embedded as a reference biometric within the credential (fingerprints reside in the Integrated Circuit Chip (ICC)).

10. The shared vision of TWIC is a high-assurance identity credential that is trusted and used across all transportation modes for unescorted physical access to secure areas and logical (cyber) access to (computer) systems.

11. The original goals of TWIC included improved security through a reduced risk of fraudulent or altered credentials by deploying biometrics to positively match an individual to a secure credential; *enhanced commerce by reducing the need for seaport workers and the trucking industry to possess multiple credentials requiring multiple background checks;* leverage current security investments; protect personal privacy by collecting minimal personal data and using a secure identity management computer system.

12. DHSMV participated in the design of TSA's Request for Proposal (RFP) process, so DHSMV was able to ensure the TSA design for vetting and credentialing would meet the requirements of § 311.12 and § 311.125, Florida Statutes.

TSA agreed to provide:

a. Up to 30 Federal enrollment centers (computers, software, communications, card production) in 12 Florida seaports;

b. A Credentialing Management System (IDMS);

c. Card Production (including printing, shipping, consumable products, etc.);

d. All necessary communications;

e. All necessary software;

f. Up to 238 perimeter ICC (Integrated Circuit Chip) biometric card entry readers;[3] and

g. 60,000 ICC Biometric cards.

To date, TSA has informed Florida that they can keep the 15 enrollment centers that were installed during the prototype phase. It is anticipated that these 15 enrollment centers will be utilized in Florida's FUPAC implementation.

13. Services and equipment promised by TSA were originally estimated to be valued at $7 to $8 million.

14. DHSMV completed the general design document for the access control system and its interface with the Federal Identity Management System (IDMS) in April 2004.

15. TSA awarded a contract to BearingPoint as the prime vendor for the development and implementation of the TWIC credentialing prototype in August 2004.

16. The 2003 state legislation specified that "By July 1, 2004, each seaport shall be required to use a Uniform Port Access Credential Card." and "Each seaport defined in § 311.09 and required to meet the minimum security standards set forth in § 311.12 shall comply with technology improvement requirements for the activation of the Uniform Port Access Credential System no later than July 1, 2004." Equipment and technology requirements for the system were specified by the department prior to July 1, 2003. The statute mandated that the system be implemented at the earliest possible time that all seaports have active technology in place, but no later than "July 1, 2004."

a. Due to the unusual partnership formed with TSA, the implementation date of this project was delayed. DHSMV provided numerous reports to Senate, House and Oversight committees to keep everyone informed that progress was being made.

17. In May 2004, DHSMV awarded a contract to ADT as its prime vendor to upgrade existing credentialing and access control systems provided to the seaports upon the original implementation of § 311.12, Florida Statutes, in 2001.

---

[2] Department of Homeland Security, U.S. Citizenship and Immigration Services, Employment Eligibility Verification, Form I–9 (Rev. 05/31/05).

[3] The placement of TSA provided readers was contingent upon seaport infrastructure readiness—only a handful of TSA readers were actually installed and those have since been removed and DHSMV provided readers will be installed.

18. Picture Perfect™, a General Electric (GE) access control product, was selected to upgrade existing GE systems previously installed in all 12 seaports—two seaports; Ft. Pierce and Port St. Joe are classified by FDLE as inactive and exempt from the credentialing and access control requirements specified in § 311.12, Florida Statutes.

19. DHSMV in consultation with the Florida Ports Council established a Seaport Implementation Committee to establish a method of communications with all seaports. Numerous meetings with each port, the Florida Trucking Association and other stakeholders have been held to continually update stakeholders on the status of the project and define the detailed design of the credentialing and access control system.

20. DHSMV also built a website dedicated to the TWIC/FUPAC program to insure seaports were versed in all aspects of the program.

21. DHSMV has completed the fee structure for the TWIC/FUPAC in accordance with Section 311.125, Florida Statutes. The fee for a four-year credential is set at $100.00 (no TSA fee was indicated by TSA since TSA does not currently have rulemaking authority to assess a credentialing fee—joint rulemaking involving the U.S. Coast Guard and TSA is ongoing and draft rules are expected to be published in the second quarter of 2006. *The readily apparent benefit to the trucking industry and other seaport workers is one credential, one fingerprint-based background check and one fee for the TWIC/FUPAC credential. Individual workers will see a substantial cost reduction with the one-time process credentialing system*.

22. TSA signed a unique partnership agreement with the State of Florida [DHSMV] which provides equipment, software, services and credentials. The intent was for the credential to be governed originally by the Florida FUPAC laws (311.125) and once TSA finalized its rules the FUPAC card would morph into a TWIC card. Because of this unique arrangement, Florida and the ports would only have to implement the credential once.

23. The TSA/DHSMV MOA provides equipment, software, services and credentials. In return Florida agreed to assist TSA in their prototype by allowing special readers to be placed in specific locations in each port. The readers have the capability to collect metrics which allow TSA to gather information. This information would assist TSA in moving forward with appropriate recommendations for final TWIC implementation. Each port has for the most part done everything possible to meet the infrastructure requirements necessary for TSA (for a variety of reasons, some seaports did not complete their infrastructure requirements in time to assist TSA in the collection of metrics. This is of particular importance since it reflects the problems seaports have in installing readers and gates. It requires ports to break concrete, install conduits and cable and build-out pedestals).

24. TSA Enrollment Centers have been installed at 12 seaports. If TWIC had been implemented in Florida seaports, the centers were necessary to capture all the applicant data along with full-face digital images, fingerprint and associated documents. This hardware setup went relatively smooth and is a credit to TSA and the TSA PMO Team.

25. TSA developed and implemented an Identity Management Data System (IDMS) in May 2005. Although TSA claimed the IDMS was in place, Florida was concerned that it was not ready for production enrollment capability. A rudimentary UAT (User Acceptance Test) was performed on May 23, 2005, with six transactions. While the six transactions were completed, the test indicated that the system was not ready for production service.

26. In June of 2005, the Florida Director, James Kneeland, test enrolled at Pensacola. The transaction was completed. However, it took over 40 minutes and had several problems associated with it.

27. In late June of 2005, TSA informed Florida that they were out of funds so they had to close the program down.

28. Florida objected and after several months of negotiation TSA agreed to conduct a User Acceptance Test (UAT) to test approximately 100 enrollments through the credentialing system. The UAT was conducted at the Port of Pensacola in October 2005, with the enrollment of 17 applicants; Port Canaveral in November, with the enrollment of approximately 17 applicants; and, Port Manatee, with the enrollment of approximately 33 applicants.

29. After a thorough analysis of the UAT data, DHSMV concluded that the functionality of the system (TWIC enrollment and identity management system) was sufficient to allow the State of Florida to work with TSA to begin the process of systematically rolling out the credentialing system to 12 deep-water seaports, provided that TSA would commit to active support of the enrollment and identity management process.

30. This recommendation was predicated on the requirement for TSA to provide support, sustainment and enhancement of enrollment software, especially, the fingerprinting component of the enrollment process.

31. A meeting was held at TSA in early December and everyone agreed to an implementation starting with Pensacola on January 9, 2006.

32. On December 29, 2005, TSA notified Florida that the implementation at Pensacola needed to be called off until further notice due to budgetary constraints.

33. Communication since December 29, 2006 has been minimal.

III. Lessons Learned/Recommendations

34. Throughout the project TSA has made numerous management changes. The lack of stability, constant change, learning curves and changing management styles has been devastating to this program. TSA needs to stabilize positions and utilize personnel who understand credentialing, access control, IT solutions and large-scale project management.

35. A lack of planning has also been devastating to this project. It was a criticism of the GAO and Florida in 2005 and it is still a major issue. It is imperative that not only should TSA partner but they should effect planning sessions with their clients and partners.

Federal Rulemaking and Background Vetting

36. TSA and U.S. Coast Guard joint rulemaking is an issue for Florida and both agencies have been briefed on Florida's concerns. It is important to recognize that under existing law in Florida, § 311.12 and § 311.125, Florida Statutes, a very high bar has been set for entry into restricted access areas and employment on the 14 public agency-owned landlord tenant congregate waterfront facilities located in the ports within the state (12 ports are actually involved in the TWIC implementation and two ports are exempt pursuant to the provisions of § 311.12, Florida Statutes.) If the TWIC requirements were to preempt existing law in Florida and if the TWIC requirements are not equally stringent the TWIC process will not "significantly improve security within U.S. ports" for the particular ports in which these public landlord tenant facilities exist because they make up a significant portion of the overall general commercial activity in the port and they make up the overwhelming majority of foreign cruise and passenger day cruise vessel activity in the ports in Florida. If the TWIC does not meet the minimums imposed by Florida law within these publicly-owned lands operating in maritime commerce security will in fact by definition be reduced. Therefore, it must be understood that for Florida the issues associated with the TWIC need to be examined both from the perspective of existing operations on private property and the security required on publicly-owned maritime landlord tenant facilities.

37. From the original concept of TWIC, the process has evolved with the intent and assurance of a high level of security to the entire process; however, the credential is only as good as the foundation documents that will tie a person to a claimed identity. Additional safeguards on the front-end process, such as verification of legal presence and work authorization for foreign nationals and verification of social security numbers, must be included in the TWIC implementation. DHSMV remains committed to work with TSA to meet these requirements during the Florida implementation phase.

38. In the future, IF TWIC is implemented in Florida, TSA and/or DHSMV should (the below recommendations also apply to the implementation of a state-issued seaport credential):

a. Provide the means to verify claimed identity foundation documents;

b. Provide a technology solution to ensure all foreign nationals applying for a TWIC have legal presence and work authorization;

c. Provide a methodology to evaluate both state of residence criminal history repository information as well as Federal (FBI) criminal history data:

—It is anticipated for the future that TSA will conduct a threat assessment check and a Federal (FBI) criminal history check that will not include the state of residence criminal history; and

—NOTE: In Florida approximately 1.5 million criminal history records are indexed at the state level that are not included in the FBI criminal history records;[4] and

d. TSA and DHSMV must provide standardized training to all trusted agent (enrollment center) personnel.

[4] Source—FDLE.

Summary

Florida is poised and ready to implement a biometric credentialing system modeled on TWIC standards and turn on the state access control system that is dependent on the biometric credential. The Florida team is committed to the implementation of a system that is effective and provides the seaports with a highly secure credentialing and access control system.

DHSMV continues to build-out the access control system; has acquired 170 handheld (portable) biometric readers and has initiated the purchase of the first-round of fixed biometric readers (and accompanying infrastructure—panels, micros, etc.) Additionally, DHSMV has developed a "fail-safe" solution that will provide for a state uniform credential that is compatible to the Federal TWIC credentialing system.

Florida will be moving forward on a parallel path to implement a Florida Uniform Port Access Credential (FUPAC) that will employ the TWIC standards. Florida remains optimistic that the Federal credentialing system and a support mechanism for the Federal system will be implemented at some point in the future and the Florida implementation will allow incorporation (within specific parameters to be negotiated) of the Federal credentialing process into the Florida system. It is now anticipated that the state implementation (roll-out) will take place beginning in mid–July 2006.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO HON. MICHAEL P. JACKSON

Question 1. How do you guarantee against duplicates or multiple identities?

Answer. As tested during prototype, the Transportation Worker Identification Credential (TWIC) Identity Management System automatically conducts a "one-to-many" search of each new applicant's fingerprints against the stored fingerprints of all previous applicants to verify that the new applicant has not previously applied for a TWIC. The final system design may be altered as required by the TWIC implementing rule.

Question 2. How do you keep aliases out of the database?

Answer. As tested during prototoype, the Transportation Worker Identification Credential (TWIC) application and vetting processes were designed to prevent an individual from using an alias to obtain a TWIC. Specific processes included:

- Digitally scanning and storing each document presented to verify an applicant's identity.
- Confirming the authenticity of passports, driver licenses, and alien registration cards through the use of a specialized document authenticator.
- Verifying the claimed identity against immigration status databases.
- Binding the claimed identity to the applicant with biometrics using both photo and fingerprints.
- Conducting a "one-to-many" search of each new applicant's fingerprints against the stored fingerprints of all previous applicants to verify that the new applicant has not previously applied for a TWIC.

The final system design may be altered as required by the TWIC implementing rule.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO HON. MICHAEL P. JACKSON

Question 1. Is it correct that if a port truck driver receives a TWIC, they will not be required to undergo an additional background check to get a Hazardous Materials Endorsement?

Answer. Yes, as proposed in the Transportation Worker Identification Credential (TWIC) notice of proposed rulemaking, that is correct.

Question 2. Where is the Department on implementing the SAFETEA–LU Hazardous Materials Endorsement background check provisions? Has the Department begun the rulemaking required by SAFETEA–LU to determine which background checks are equivalent to the Hazardous Materials Endorsement background check?

Answer. The Transportation Security Administration (TSA) has proposed standards to determine the comparability of other governmental background checks in the Transportation Worker Identification Credential (TWIC) proposed rule, which was published May 22, 2006. The proposed rule also states that the background check

administered by the U.S. Customs and Border Protection (CBP) Free and Secure Trade (FAST) program and the hazardous materials threat assessment are comparable. After reviewing comments and making any necessary changes to the proposed rule, TSA will publish a final rule that includes comparability standards and comparability determinations.

Question 3. As you may know, Section 7105 of SAFETEA–LU requires states that have additional background check requirements for Hazardous Materials Endorsements provide due process procedures for applicants identical to those offered to applicants undergoing the Federal background check. Will DHS require states that develop their own security credentials above and beyond TWIC to provide the same due process procedures for applicants as the Federal Government provides applicants under the TWIC application process?

Answer. The Transportation Security Administration (TSA) issued a proposed rule for the Transportation Worker Identification Credential (TWIC) on May 22, 2006, held four public hearings, and is currently assessing comments from the industry and public. Therefore, we cannot determine at this time what the final TWIC standards will require. Federalism concerns may prevent the Department of Homeland Security (DHS) from requiring certain specific state actions.

Question 4. Can you explain the individual components that make up the roughly $100 cost of a TWIC (Transportation Worker Identification Credential) that is charged to hazmat-endorsed truck drivers? Since they already have a background check that satisfies the requirements of TWIC, what else must they pay for beyond the card itself?

Answer. As described in the Notice of Proposed Rulemaking for the Transportation Worker Identification Credential (TWIC), TSA estimates that applicants who already have a Hazardous Materials Endorsement will be charged an estimated $105 for a TWIC. The components of those costs are as follows:

Enrollment/Issuance—	$55
Credential Production—	$50
Total—	$105

The Threat Assessment estimated cost, including the $22 paid to the Federal Bureau of Investigation (FBI) for its Criminal History Records Check (CHRC) and paid by applicants without a comparable background check, is not assessed to applicants with a comparable current background check.

Question 5. Are the truck driver fingerprints collected through the Hazardous Materials Endorsement background checks retained by the Transportation Safety Administration (TSA)? Can these fingerprints be used for the TWIC application or will drivers have to be re-printed?

Answer. The Transportation Security Administration (TSA) retains only those fingerprints collected by the TSA agent in 33 states and the District of Columbia. Seventeen states collect fingerprints using existing state infrastructures and may or may not store fingerprints. Regardless of the availability of fingerprints from sources other than the Transportation Worker Identification Credential (TWIC) enrollment process, good business practice is to maintain a chain-of-trust for all data that requires the collection of identity documents and biometric data (photo and fingerprints) during a single, seamless enrollment process. This process avoids potential data file matching errors and conforms to the Personal Identity Verification procedures required by Federal Information Processing Standard (FIPS) 201–1. Since all TWIC applicants must be present to enroll, the incremental time and cost to collect fingerprints with the scanning device during enrollment is small.

Question 6. Under the Coast Guard's Maritime Identification Credentials program announced in the *Federal Register* on April 28, 2006, port workers and sailors needing unescorted access to secure port areas are required to undergo name-based background checks to receive a credential until the TWIC (Transportation Worker Identification Credential) program is implemented. I understand port truck drivers, who make up one of largest segments of port workers and have access to most areas of a port, are exempt from this requirement. Can you explain why?

Answer. The Coast Guard's Maritime Identification Credentials program was an interim security measure at our ports. It was not intended to replace the Transportation Worker Identification Credential (TWIC) nor was it intended to capture the entire maritime port worker population. Long-haul truckers, due to their high degree of mobility, were not included in this measure. The measure targeted those populations within the more direct control of port facility and vessel operators. Name-based background checks are an immediate security measure designed to

limit individuals that pose a threat from gaining access to port facilities. This is a first step that covers those individuals with frequent access to our ports. Other populations are expected to be covered when the TWIC program is fully implemented.

Question 7. If it was deemed too difficult to require name-based background checks for port truck drivers under the Maritime Identification Credentials program, how will the Transportation Security Administration (TSA) handle fingerprint-based background checks for port truckers when TWIC is implemented?

Answer. All workers requiring a Transportation Worker Identification Credential (TWIC) will enroll in exactly the same manner at enrollment sites operated by TSA through contract arrangements.

Question 8. Based on your testimony, you say that the TWIC pilot project awarded to BearingPoint has proven that the TWIC technology can work in the field. Yet the Delaware Exchange testimony indicated that the biometric was never tested in the pilot and the interoperability of the pilot was tested in limited circumstances. How do you account for the failure to test biometrics and the cards interoperability and still claim the pilot was successful?

Answer. During prototype, biometric readers were tested at selected maritime facilities in the three prototype test areas: Delaware River Valley; Florida; and Los Angeles/Long Beach. Biometric readers were tested at maritime facilities in Florida and LA/LB. Readers matched the fingerprint template on the prototype card to the template generated by the fingerprint scanning pad on the reader. Since the Transportation Worker Identification Credential (TWIC) prototype tests, the National Institute of Standards and Technology (NIST) has specified the fingerprint template biometric as the standard for all government employee Personal Identity Verification (PIV) credentials. The interoperability of the TWIC with a wide variety of readers is assured since TWIC will follow the technical standards set by NIST for all government PIV credentials.

Question 9. The TWIC pilot project contract was originally to include 75,000 workers at a cost of $12.3 million. However, according to the August 2005 BearingPoint Report it ended up including only 1,657 cards, costing $22.8 million. The pilot project was over budget and undersubscribed. How can you say this pilot was successful when only 1,657 cards were used in the field?

Answer. The objectives achieved during Phase III of the Transportation Worker Identification Credential (TWIC) Prototype Program were to: (1) assess performance of conceptual TWIC identity management business processes; (2) assess performance of TWIC as an access control tool; and (3) assess readiness of TWIC system for production phase. The Transportation Security Administration (TSA) concluded that the TWIC prototype system is functional and met all requirements specified for the prototype. TSA has concluded that the TWIC prototype business processes demonstrated the capability to meet each of the broad objectives of the TWIC mission-need statement.

Question 9a. Further your testimony claims over 4,000 cards were tested. What date are you drawing this metric from? What was the cost of the sustaining the BearingPoint contract to this date?

Answer. Following the conclusion of prototype testing on June 30, 2005, the Transportation Security Administration (TSA) continued to enroll workers and issue prototype Transportation Worker Identification Credentials (TWIC) to support those facilities that participated in prototype and wished to continue using the TWIC for their access control systems. By the time TSA concluded this support to prepare the system for implementation, over 4,000 cards had been issued to workers. During this extended period, TSA gained additional confidence in the TWIC system's ability to routinely enroll workers and provide them with credentials quickly and efficiently. As of May 31, 2006, $26.3 million had been expended on the BearingPoint prototype contract.

Question 10. How does TSA and the Coast Guard plan to administer their responsibilities for processing TWIC cards and Merchant Mariner Documents (MMD)? Will the Coast Guard be processing an application for an MMD at the same time that TSA is processing the TWIC application or will the Coast Guard wait to process a MMD until after TSA completes the vetting process for a TWIC card? How will TSA be notifying the Coast Guard when a TWIC background check is completed? What specific functions of an MMD application is being transferred to TSA?

Answer. It is the Coast Guard's intent to obtain identity data from TSA and use it to process mariner applications for Merchant Mariner Credentials. The Merchant Mariner Credential (MMC) would take the place of the current merchant mariner license, document and Certificate of Registry, so the Coast Guard would be issuing an MMC and no longer issue the MMD referenced in the question above. In the Notice of Proposed Rulemaking (NPRM) published in May, the Coast Guard proposed

to begin processing MMC applications only after an individual was issued a TWIC. In the public meeting process, the Coast Guard and TSA received many comments about the current delay in the MMD/Licensing process and the concern that the public has with respect to adding a TWIC processing time onto that process. All of these comments will be addressed in the final rule.

Question 12. How does the Coast Guard plan to apply TWIC card verification procedures on vessels? How is a secure area defined on vessel? Does this restrict vendors, contractors from access to a vessel for people performing minor repairs unless they have a TWIC card?

Answer. The Coast Guard and Transportation Security Administration are reviewing comments received in response to the joint notice of proposed rulemaking. It would be inappropriate at this time to provide a detailed response because the rulemaking process is ongoing. The final rule will address TWIC verification onboard vessels and at facilities. There will be clarification regarding the areas where TWIC will be required.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO LISA B. HIMBER

Question 1. Would you explain what you see as the biggest vulnerabilities at your port facility that need to be addressed?

Answer. The Maritime Exchange for the Delaware River and Bay does not represent a single port facility; rather we represent each of the facilities operating in the port region, including both public- and private-sector, handling general cargo, containers and petroleum facilities in each of the three states bordering the Delaware River. Accordingly, the answer to this question will be specific to those vulnerabilities associated with access control rather than other potential areas of exposure or weakness.

An attack against a vessel docked at a maritime facility, particularly an oil, gas or chemical tanker, would certainly result in a major disruption to Delaware River Port operations. Undoubtedly we could expect a cessation of all port activities for many days or weeks. A larger concern from a public health and safety perspective surrounds a shore-based attack on the facility itself (*e.g.,* someone driving a truck laden with explosives into a facility). An event of this scope has the potential for much greater impact on the surrounding population than would an attack against a single vessel.

Additionally, under MTSA, facility security officers (FSOs) are required to ensure that everyone entering their facilities has the right and the need to do so. That there is no standard, effective system in place to provide FSOs with advance notice of gate schedules—or modifications to those schedules—leaves a security hole. Obviously, the operations at each trucking company or facility will be unique to its needs, and such an advance notification system may not be practical in every instance. Yet in many instances. not only are some FSOs unaware of who is planning to arrive on any given day to drop off or pick up cargo, but when those individuals reach the facility. there are many who are unknown to security personnel.

Most facility operators in the Delaware River region require a U.S. or Canadian driver's license at a minimum, and all truck drivers will have paperwork authorizing them to pick up (delivery order) or drop off (booking), but there are no guarantees that these documents are legitimate or that the individuals have undergone security screening.

Another vulnerability exists waterside at some facilities. In reality, many facility operators have no advance information on what crew members—U.S. or foreign—will be arriving on vessels docking at their facilities. In many instances, facilities are not provided with crew/non-crew manifest at any point during the vessel call. If ships are coming from foreign, FSOs must rely on an advance screening of these persons by U.S. Customs and Border Protection. If an individual is deemed to be high-risk, CBP and Coast Guard will require that the vessel owner (or operator/agent) hire a security guard or take other appropriate measures to ensure the individual does not attempt to debark the vessel. The facility operator is not necessarily privy to this information.

Facility and vessel owner/operators would prefer that if an individual is deemed high-risk, he be escorted off the vessel/facility by appropriate Federal personnel.

Question 2. How far would implementation of the TWIC go toward mitigating those vulnerabilities?

Answer. While it would not completely eliminate the vulnerabilities described above, the TWIC will go a long way toward minimizing current susceptibilities. With the exception of aliens arriving by vessel (or indeed foreign seafarers arriving

via land to join a ship) who are exempted from the TWIC program as proposed May 22, with the TWIC program in place FSOs would have the assurance that the individuals arriving at their facilities have undergone security screenings. This would provide a measure of expectation that the individual is less likely to attempt a terrorist action, or otherwise tamper with, steal, or mishandle vessels, containers and cargoes moving through U.S. seaports.

This assurance is further heightened due to the fact that TWIC is designed to be used in conjunction with a biometric identifier and is in fact a tamper-proof credential.

Used in conjunction with other programs mandated under the Maritime Transportation Safety Act or individual vessel/facility security plans. it is expected that TWIC will be a valuable tool to harden access control to U.S. ships and facilities.

Currently, it is anticipated that foreign seafarers will be exempted from the TWIC regulations when they are promulgated.

Question 3. Why has it taken so long for the Federal Government to implement the TWIC and what improvements would you recommend that the government make?

Answer. With regard to the first part of the question. one can only speculate. As indicated in the written and oral testimony presented May 16, I believe a large part of the delay has resulted from the continual changes in program management—from leadership at all levels down to the day-to-day operating staff. The largest gap in the TWIC deployment schedule seemed to be between the end of Phase II, the Technology Evaluation, in October of 2003 and commencement of Prototype in November of 2004. I believe it was during this time that questions surfaced as to whether TSA should issue a standard or manage the program, but I do not know whether there were other factors involved which postponed the schedule so dramatically. It appears reasonable to assume that the learning curve faced by the new personnel within the TSA program office, coupled with the fact that TSA utilized different contractors for Phase III than were involved in Phase II, may have prolonged the delay.

I also believe there was another unexpected setback associated with a modification of the contract for the TWIC Prototype Phase after it had been awarded: I was apprised neither of the scope of the modification nor the reasons for making the change. Last, I understand there was a suspension of activity in late 2004, early 2005, while the card production activities were moved mid-process from a facility in Pennsylvania to one in Kentucky. I am not aware of why the decision was made to start the process in Pennsylvania or why it was moved once started.

I am unfamiliar with the level of technical and operational training made available to both program managers and "trusted agent" contractors, but I believe many individuals involved in the pilot program experienced significant delays associated with improper use, operation, and performance of the system.

With regard to improvements that can be made, I offer the following:

A. Program Management

- To ensure future delays are minimized, or at least the effects of such delays are mitigated, it might be appropriate to create a Government-Industry Oversight Committee to work with TSA and address issues as they arise during the implementation period.
- TSA should also establish a consistent and clear method of communicating information to government and industry stakeholders.
- DHS must identify a mechanism to ensure program and contractors management and staff personnel will remain with the program through implementation.
- Program staff must undergo sufficient training to ensure they can operate the system effectively. If necessary, technical personnel should be available onsite to address any system deficiencies within a reasonable time-frame. In many offices, for example, IT contractors must guarantee a response time of not more than 4 hours. TWIC personnel must also be conversant with the regulations governing the program and its myriad processes (such as, who is required to obtain a TWIC, background checks, how to request an appeal, etc.) to ensure they can answer applicant's questions in a timely and accurate manner. Along these lines, TSA and Coast Guard should develop a joint Frequently Asked Questions (FAQ) document.
- The U.S. should work through the International Labor Organization to ensure that all mariners be in a position to provide electronic verifiable credentials which are compatible with TWIC. If the ILO adopts a technology which is incompatible with TWIC, the U.S. must be prepared to adopt the international technology in a reasonable, low-cost time-frame.

B. Program Operation

- Test the technology—more below.
- TSA should modify the web portal to allow for additional automation of TWIC tasks. For example, the TWIC portal could be used to request a replacement card rather than a personal visit.
- TWIC can serve as a building block for a host of programs which will improve security while facilitating commerce at U.S. seaports and in other modes of transportation. For example, it can serve as the basis for an advance terminal gate appointment system as described above, it can be used to tie a truck driver to a company, which can then potentially be tied to an electronic version of a cargo delivery order. This electronic delivery order could likewise be linked electronically to the cargo manifest provided by the ocean carrier to the facility operator, further strengthening the security of the cargo supply chain once the cargo lands in the U.S.
- TSA should add the capability for applicants to request access at multiple facilities at time of enrollment. TWIC holders might also use the TWIC portal to request access to any facility to which they've not been granted access previously. This will go a long way toward minimizing the amount of time spent entering data into the facility internal access control systems upon first arrival.
- Some operators require color codes to visually determine that an individual has rights to be in a certain part of the vessel or facility (or warehouse, railyard, etc). TSA should work with industry to identify mechanisms which may be used to visually identify individuals via the TWIC.
- During the pilot program. there were times when the applicant was not notified that the enrollment center had received the card from the production facility. We suggest TSA include e-mail notifications to the applicant when the card is shipped to and received at the enrollment center.
- Because mariners and truck drivers are often away from their homes for extended time-periods, the TWIC program should offer applicants an option to designate an enrollment center for card pick-up or mail the card to their homes or workplaces rather than requiring they to return the center where the applications were originally processed.
- In addition to testing the technology. TSA needs further testing on the processes associated with using a TWIC before it can be deployed at maritime facilities on any wide scale. For example, the card hotlisting, revocation and notification processes were not tested, neither was the individual applicant enrollment (vs. employer sponsor enrollment of employees). There are undoubtedly many other additional opportunities for improvement that may present themselves during the next testing phase.

An opportunity exists to address the vulnerability mentioned above regarding facility operators' lack of advance information on which crew members will be arriving at their facilities on vessels. This opportunity is not available via TWIC, but rather through another DHS program: the Coast Guard electronic Notice of Arrival/Departure (eNOA/D) system.

Under current regulations, vessel owners or operators must submit detailed crew manifest data not less than 96 hours prior to each vessel's arrival in the U.S. The Maritime Exchange and others have requested on numerous occasions that CBP and Coast Guard provide local port community information systems with copies of that eNOA/D data. This request has precedent in the CBP "Port Authority Download" component of the Automated Manifest System. In short, a certified entity in a local port, such as a Maritime Exchange or Port Authority, can receive electronic copies of all manifest data filed by ocean carriers for ships destined for their ports.

We believe adding similar functionality to the eNOA/D system would provide a secure, effective means for the Federal Government to share critical data with the private sector, and as illustrated above, fill a security gap. To date, however, the Coast Guard has declined requests to partner on this initiative.

Question 4. Do you believe the technology necessary for implementing the TWIC at port facilities—card readers, etc.—is ready for deployment?

Answer. No.

As indicated during my September 16 testimony, there were many technical components—and associated processes—that were either untested or under-tested during the TWIC pilot program. These include the TSA-vessel/database facility electronic communications (database updates to facilities, notification to TSA by facilities of who has been granted access, and subsequent hotlisting notifications) and

processes; use of a biometric and/or pin number for access in a maritime environment, validation of identification documentation provided at enrollment.

Further, that the use of TWIC was not tested on vessels, which will rely on wireless telecommunications access, is troubling. Additionally, that the card used during the Pilot program did not meet the FIPS–201 standard required by Homeland Security Presidential Directive 12 and that the card formally deployed must do so, is also a significant concern. Changing out the underlying technology in essence negates all aspects of the TWIC pilot program beyond initial application processing.

We appreciate the August 16 announcement by TSA and Coast Guard that they would change the approach to TWIC deployment to address card issuance processes in the first phase and holds off on infrastructure (*i.e.,* card readers) installation and usage to a second phase. However, as welcome as this approach may be, it does present a distinct possibility that cards issued during Phase I will not operate in the technology ultimately selected for Phase II.

Recently, the U.S. Maritime Administration Ship Operations Cooperative Program, has successfully tested its Mariner Access Card, which will use technologies and processes similar to those proposed for TWIC. The initial reports are very positive, and we are optimistic that the technologies proposed will work in the maritime environment. However, this has yet to be used in any operating capacity and we therefore remain concerned that TSA does not deploy a full-scale roll-out without additional testing.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO GEORGE P. CUMMINGS

Question 1. Much was made in Congress about the proposed acquisition of U.S. port terminal leases by Dubai Ports World. Would the controversy have been nullified had the TWIC program been in place?

Answer. Implementation of the TWIC program would have mandated that all individuals to be granted unescorted access to the restricted areas of the terminal would have to qualify for a TWIC card, regardless of their position in the company. This would have ensured that all of these individuals were legally present in the United States.

Question 2. From your experiences regionally, what are the greatest impediments to nationwide implementation of TWIC?

Answer. The selection of the technology to be used in the card readers will be critical. The technology identified in the Notice of Proposed Rulemaking would have required a full contact card and a PIN number for each entry. This would have caused major delays at terminal gates. We were in agreement with the recent change to the proposed regulation to delay the requirement for installation of card readers at facilities until a system is identified that can read cards and biometrics rapidly enough that back-ups do not occur at marine terminal gates.

Also, there may be a significant impact to the population of truck drivers that haul containers in and out of the port if a large number of these drivers are not eligible for the TWIC card.

○