AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–1071

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) IMPLEMENTATION

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

APRIL 12, 2007

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

U.S. GOVERNMENT PRINTING OFFICE

39–014 PDF WASHINGTON : 2010

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 TENTH CONGRESS

FIRST SESSION

DANIEL K. INOUYE, Hawaii, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska, *Vice Chairman*
JOHN F. KERRY, Massachusetts	JOHN MCCAIN, Arizona
BYRON L. DORGAN, North Dakota	TRENT LOTT, Mississippi
BARBARA BOXER, California	KAY BAILEY HUTCHISON, Texas
BILL NELSON, Florida	OLYMPIA J. SNOWE, Maine
MARIA CANTWELL, Washington	GORDON H. SMITH, Oregon
FRANK R. LAUTENBERG, New Jersey	JOHN ENSIGN, Nevada
MARK PRYOR, Arkansas	JOHN E. SUNUNU, New Hampshire
THOMAS R. CARPER, Delaware	JIM DEMINT, South Carolina
CLAIRE MCCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	JOHN THUNE, South Dakota

MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
LILA HARPER HELMS, *Democratic Deputy Staff Director and Policy Director*
CHRISTINE D. KURTH, *Republican Staff Director, and General Counsel*
KENNETH R. NAHIGIAN, *Republican Deputy Staff Director, and Chief Counsel*

CONTENTS

	Page
Hearing held on April 12, 2007	1
Statement of Senator Carper	30
Statement of Senator DeMint	55
Statement of Senator Inouye	1
Prepared statement	2
Statement of Senator Lautenberg	3
Statement of Senator Smith	5
Statement of Senator Stevens	3

WITNESSES

Hawley, Hon. Edmund S. "Kip", Assistant Secretary, Transportation Security Administration, DHS	5
Prepared statement	7
Himber, Lisa B., Vice President, Maritime Exchange for the Delaware River and Bay	34
Prepared statement	36
Pomaikai, Sr., Capt. Paul Kaipo, Assistant Port Captain, Sause Bros.; on behalf of the American Waterways Operators	42
Prepared statement	44
Rabkin, Norman J., Managing Director, Homeland Security and Justice Issues, GAO	16
Prepared statement	18
Rodriguez, Michael J., Executive Assistant to the President, International Organization of Masters, Mates and Pilots, AFL–CIO	47
Prepared statement	48
Salerno, Brian, Rear Admiral and Director of Inspections and Compliance, USCG, DHS	13
Prepared statement	14

APPENDIX

Maritime Trades Department, AFL–CIO, prepared statement	64
Passenger Vessel Association, prepared statement	62
Response to written questions submitted by Hon. Maria Cantwell to:	
Hon. Edmund S. "Kip" Hawley	74
Capt. Paul Kaipo Pomaikai, Sr.	89
Norman J. Rabkin	85
RADM Brian Salerno	82
Response to written questions submitted by Hon. Daniel K. Inouye to:	
Hon. Edmund S. "Kip" Hawley	67
Lisa B. Himber	87
Capt. Paul Kaipo Pomaikai, Sr.	88
Norman J. Rabkin	84
Michael J. Rodriguez	89
RADM Brian Salerno	81
Response to written questions submitted by Hon. Frank R. Lautenberg to:	
Hon. Edmund S. "Kip" Hawley	71
Lisa B. Himber	87
Michael J. Rodriguez	91
RADM Brian Salerno	83
Response to written question submitted by Hon. Bill Nelson to Hon. Edmund S. "Kip" Hawley	79

Page

Response to written questions submitted by Hon. Ted Stevens to:
Hon. Edmund S. "Kip" Hawley 71
Norman J. Rabkin 85
Response to written questions submitted by Hon. David Vitter to Hon. Edmund S. "Kip" Hawley 80
Wells, Ken, President, Offshore Marine Service Association, prepared statement 59

TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) IMPLEMENTATION

THURSDAY, APRIL 12, 2007

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

The Committee met, pursuant to notice, at 10:00 a.m. in room SR–253, Russell Senate Office Building, Hon. Daniel K. Inouye, Chairman of the Committee, presiding.

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

The CHAIRMAN. The Transportation Worker Identification Credential program, the TWIC, has been under development since 2001, and despite $99.4 million in appropriations from Congress, unfortunately the program still is languishing at the Department of Homeland Security.

In our last hearing on this subject about a year ago, we heard testimony about severe cost over-runs, contract mismanagement, excessive personnel turnover, poor communications and ineffective planning. At this hearing, we will examine whether the Transportation Security Administration and the United States Coast Guard have taken actions to address those criticisms.

Additionally, I hope to hear how the agencies plan to deploy the biometric card enrollment and issuance process, just as importantly, how the agencies plan to execute the pilot program for card-reader technology.

While I do not want to dwell on the mistakes of the past, this Committee needs assurance that the Administration has taken seriously the mismanagement of the TWIC program. Given that comprehensive management plan for TWIC required in the Intelligence Reform Act of 2004 is over two years past due, I can only conclude that the Administration is not taking its responsibility seriously enough. If the agencies continue to neglect the basic tenets of contract management and programmatic planning, failure is certain to follow.

Completion of this program is a crucial step towards improving the security of our ports. And so, failure is unacceptable.

When Congress considered the SAFE Port Act, we established implementation deadlines in consultation with the Department of Homeland Security. We did not want to impose a set of deadlines that the agencies would not be able to achieve. Working collaboratively, we required TWIC enrollment at the Nation's top ten high-risk ports by July 1, 2007. As of today, we do not have even

the most basic deployment schedule. However, I am informed that enrollment scheduled to begin in Wilmington, Delaware, in late March has been postponed until late May, at best.

We are all concerned that the low estimates of the population affected by the program are not realistic. This estimate is significant, in that it will determine the number of enrollment stations the contractor sets up and the number of trusted agents the contractor hires to process employees. An underestimate of the affected population would thus cause a domino effect, resulting in long wait times at the enrollment stations, poor customer service, and ultimately a slowing of the flow of commerce as labor circulates through a clogged enrollment and card issuance process.

As we move forward with testing and implementing card-reader technology in the rough maritime environment, the TSA and the Coast Guard must appropriately balance their multiple missions of safety, security and efficiency for both facilities and vessels. The card reader system cannot slow the flow of commerce through our terminals. The security practices the Department puts into place cannot compromise crew safety.

I can appreciate the challenges associated with addressing these divergent issues. It is a difficult balancing act. However, after six years and $99.4 million, we still do not have access controls in our ports. I'm certain all agree that we need to get this program on track, and on schedule, for the safety and security of our Nation.

[The prepared statement of Senator Inouye follows:]

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

The Transportation Worker Identification Credential (TWIC) program has been under development since 2001 and despite $99.4 million in appropriations from Congress, it is still languishing at the Department of Homeland Security.

In our last hearing on this subject almost 1 year ago, we heard testimony about severe cost-overruns, contract mismanagement, excessive personnel turnover, poor communications and ineffective planning. At this hearing, we will examine whether the Transportation Security Administration (TSA) and the United States Coast Guard have taken actions to address those criticisms.

Additionally, I hope to hear how the agencies plan to deploy the biometric card enrollment and issuance process, and just as importantly, how the agencies plan to execute the pilot program for card reader technology.

While I do not want to dwell on the mistakes of the past, this Committee needs assurance that the Administration has taken seriously its mismanagement of the TWIC program. Given that the comprehensive management plan for TWIC required in the Intelligence Reform Act of 2004 is over 2 years past due to Congress, I can only conclude that the Administration is not taking its responsibility seriously enough. If the agencies continue to neglect the basic tenets of contract management and programmatic planning, failure is certain to result. Completion of this program is a crucial step toward improving the security of our ports. Failure is unacceptable.

When Congress considered the SAFE Port Act, we established implementation deadlines in consultation with the Department of Homeland Security. We did not want to impose a set of deadlines that the agencies would not be able to achieve. Working collaboratively, we required TWIC enrollment at the Nation's top ten high risk ports by July 1, 2007. As of today, we do not have even the most basic deployment schedule. I am informed that enrollment scheduled to begin in Wilmington, Delaware, in late March has been postponed until late May, at best.

I am also concerned that the low estimates of the population affected by the program are not realistic. This estimate is significant, in that it will determine the number of enrollment stations the contractor sets up and the number of trusted agents the contractor hires to process employees. An underestimate of the affected population would thus cause a domino effect, resulting in long wait times at the enrollment stations, poor customer service, and ultimately a slowing of the flow of

commerce as labor circulates through a clogged enrollment and card issuance process.

As we move forward with testing and implementing card reader technology in the rough maritime environment, the TSA and the Coast Guard must appropriately balance their multiple missions of safety, security and efficiency for both facilities and vessels. The card reader systems cannot slow the flow of commerce through our terminals. The security practices the Department puts into place cannot compromise crew safety.

I can appreciate the challenges associated with addressing these divergent issues. It is a difficult balancing act. However, after 6 years and $99.4 million, we still do not have access controls in our ports. We need to get this program on track, and on schedule, for the safety and security of our Nation.

Senator Stevens?

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

Senator STEVENS. Thank you, Mr. Chairman. I will have to leave here almost immediately, but I did want to stop by and state that I am encouraged that some progress has been made on this Transportation Worker Identification Credential, TWIC, since our hearing took place a little over a year ago. In January, I understand the final rules were issued for the biometric smart card to be used in the TWIC program. The Coast Guard is developing a process for expedited temporary clearance for newly-hired port and vessel workers. And, stakeholders indicate that communication within the Transportation Security Administration, TSA, has improved significantly. There is, however, room for improvement.

Over four years have passed since the first legislative mandate requiring the development of this program, TWIC. Most recently, the SAFE Port Act established a timeline for deployment of the program to begin at 10 ports no later than July of this year. It is now my understanding that this statutory deadline, which was developed in coordination with the Department of Homeland Security and TSA, will likely not be met.

Our Nation's ability to secure our ports largely rest in part on our ability to timely verify and identify our port workers and to prevent unauthorized access to these secure maritime areas.

Absent this ability, port operations will remain at risk. The program is a complex undertaking. TSA and the Coast Guard and others are trying to ensure that we do have secure port operations. The Congressional tolerance, I'm sure you're aware, is waning because of the missed deadlines.

I do have to leave, as I said. I look forward to reviewing the testimony from our witnesses, particularly their suggestions on how to get the program back on track and keep it on track.

Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thanks, Mr. Chairman.

Thank you. Not to be repetitious, but as I listened to the Chairman's statement, we are talking about similar things, in our views, and we can't leave this situation as it is. It presents too many risks for our society. And, so when we talk about the failures of the past,

it's simply to make sure that we understand what hasn't taken place that should have taken place. And, to get an examination of what's required. That's the most important thing.

The Delaware River port system in South Jersey is the busiest crude oil tanker port in the United States and it's the third busiest in the world. The Port of New York and New Jersey is the largest port on the East Coast and it's the second busiest container port in the country. And, Northern New Jersey's port sits alongside an area that has been defined as the two most dangerous miles in America for terrorism, according to the FBI.

Now, New Jersey's ports are vital to our region, not only vital to our region, but our national economies as well. And, the security of the vessels that dock there, longshoreman who work there and surrounding communities are even more critical to me. It's an area that is home to—whether during their business or residential hours—to approximately 12 million people. So, we've got to be very arduous in terms of getting this program underway, it's essential.

The White House has had a chance to demonstrate their commitment to port security by getting the TWIC program up and running. But, instead of making this program a success, the Administration has let it become another example of mismanagement, poor planning, and neglect of our Nation's security.

Almost 6 years after 9/11, only 1,700—one thousand seven hundred—are known to be in the hands of cardholders, that's after 6 years, almost 6 years. And the Bush Administration has spent, as the Chairman said in his comments, nearly $100 million administering this program. That, my friends, is nearly $60,000 a card they've spent.

With so many workers lacking their TWIC cards, the Bush Administration tried to conduct more basic security measures by running the names of port workers against the Nation's Terror Watch List. But, while the Administration did background checks on dock workers with access to secure areas of the port, they failed to check truck drivers—so numerous—with access to the same secure areas of the port.

With the help of Chairman Inouye and Vice Chairman Stevens, I secured language in last year's SAFE Port Act, to require them to include truck drivers, to get this right, by January 2007. But, thus far, the law has been ignored by the Administration. And now, to try and get TWIC back on track, the Administration wants to charge employees for their IDs, at a cost of $135 apiece.

Worse still, we have no assurance that our ports will have the technology to scan these biometric cards, because the President didn't request any funding for it. This kind of mismanagement is not fair to our workers, it's not fair to our ports, it's not fair to our communities, and it's not the level of security that we need in our country.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Senator Smith?

STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH. Thank you, Mr. Chairman, for all your good work, and for holding this hearing.

I thank our witnesses, also, for being here today. It has been a long road getting to this point.

When we first mandated the issuance of the biometric transportation security card, known as TWIC, as part of the 2002 Maritime Transportation Security Act, I was—at that time—the Ranking Member on the Surface Transportation and Merchant Marine Subcommittee. After a hiatus of 4 years, I'm once again the Ranking Member. And, unfortunately, we're still dealing with the TWIC program implementation.

No question, there have been mistakes along the way and it's understandable given all of the difficulties and complexities of starting up a Department like Homeland Security. The fact remains, that we're entrusted as stewards of the public's fiscal resources, and more importantly, in providing for the safety and security of the American people.

The SAFE Port Act mandated the Transportation Security Administration rollout the TWIC program at 10 U.S. ports later this year. The Port of Portland, in my home State of Oregon is not one of those ports selected for the initial phase, the roll-out, but I'm told the Port's Maritime Security Manager is meeting with the TWIC contractor this morning to talk about the implementation schedule for Portland. So I, along with folks back home in Oregon, am watching this phase of the roll-out very closely with the expectation that it will soon be Portland's turn.

I believe that TWIC is an important program, and it's important to get it right, so for that reason, I know we're holding this hearing, and again, I thank you for that, Mr. Chairman.

The CHAIRMAN. Thank you very much. This morning we have two panels, the first panel consists of the Assistant Secretary of Transportation Security Administration, Mr. Ed "Kip" Hawley, from the United States Coast Guard; Rear Admiral Brian Salerno; and the Managing Director of the Homeland Security and Justice Issues, Government Accountability Office, Mr. Norman J. Rabkin.

And, I call upon Secretary Hawley.

STATEMENT OF HON. EDMUND S. "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION, DHS

Mr. HAWLEY. Good morning, Mr. Chairman, thank you and members of the Committee, Ranking Member Smith. Thank you for this opportunity to discuss the TWIC program. I'm pleased to be here this morning with Admiral Brian Salerno, our partner from the Coast Guard, and Norm Rabkin from the Government Accountability Office.

I'd like to spend a little bit of time talking in detail about the program overall, its technology, business process and timetable. But to start off, I think I should answer one fundamental question, which is why is this taking so long?

In a city where most of us wear one or more security ID cards, what is so hard about producing a TWIC? There are four major differences from this kind of a card.

First, TWIC uses the latest, most advanced Federal Government biometric standard, and for the first time, applies it to the commercial sector. Second, TWIC issues cards that work anywhere in the Nation's private port environment, by anyone working there, across companies, and industries. Third, TWIC has not only unparalleled flexibility, it has massive scale. Somewhere in the realm of 1 million cardholders in 3,200 ports. In comparison with our prototype project, we will process in one day, more credentials than we did in one year, under the prototype.

Finally, TWIC security checks will be integrated into all of TSA's vetting programs, which means that we can connect the dots throughout the entire transportation sector. TWIC is an advanced, sophisticated, credentialing system. In other words, the hard part is not the card, it is the network behind the card.

Breaking new ground in technology has obvious advantages, but it always brings schedule risks, and TWIC is no different. Three developments in the last year have made this project even more complex. First, we made the decision to bring TWIC into alignment with a new Federal Government biometric standard called FIPS 201. Second, we identified and closed potential data privacy gaps, as of this past February. And third, working with the Coast Guard, we incorporated more than 1,900 comments received during our rulemaking process, into the detailed blueprint for TWIC. That rule became final several weeks ago.

On top of the challenges I mentioned of introducing new technology on a massive scale, while at the same time, making the three major program adjustments, we have one more additional complexity, and it is a big one. We will connect TWIC into what we call the screening gateway.

As you know, TSA vets many different people in different industries—aviation, truck drivers, now maritime—and in order not to miss potential links among them, we now use a centralized vetting system. So, in turning TWIC on, we must be absolutely certain that we do not jeopardize the stability or security of this larger vetting system. The only way to be sure is to flight-test TWIC extensively.

All of the internal moving parts to TWIC must work together, and they must work in combination with the larger screening gateway. Rigorous performance testing is the only way to know for sure that TWIC is ready to go live. That's where we are in the process, and what remains is the testing.

Everybody wants to know when TWIC enrollments will start, and we are all very mindful of the SAFE Port Act deadline of July 1 to enroll 10 ports in TWIC. So, where are we on that?

TSA has already conducted—as Senator Lautenberg mentioned—Watch Lists and immigration checks for over 750,000 port workers, and will do it again over the Summer to keep that assessment fresh. I believe that addresses the near-term, real-world security concerns about the current workforce, even before the cards are issued.

For us, the stakes are enormously high. For the people who pay for these cards, and use them daily to enter workplaces and jobs,

they are also high. Out of respect for these employees and the businesses, we must spend the time to ensure that the program is tested, fully integrated, and does not compromise security in any linked system.

We respect the deadline, and April is too soon to give up on a July deadline. But, if it is a choice between meeting that deadline, and program integrity, we will choose the latter.

We have a strong new team onboard from Lockheed Martin with excellent program support from TSA and the Coast Guard. The industry and its workers have been forthcoming and constructive. For commerce, TWIC means that thousands of independent businesses will have one, interoperable security network for the first time in history.

We look forward to working with the Committee to ensure the success of the TWIC program, and port security, generally.

Thank you for the opportunity, I'd be happy to answer questions.

[The prepared statement of Mr. Hawley follows:]

PREPARED STATEMENT OF HON. EDMUND S. "KIP" HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION, DHS

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

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

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

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

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

Achieving these ambitious goals has required creative planning, flexible implementation, effective stakeholder communication, and adaptive contract management. The basic program deployment philosophy has been a commitment to evaluate all practicable technical alternatives that will provide adequate port security and minimize adverse impacts, either economically or logistically, to our Nation's citizens and our international trading system. This has been and will continue to be the program's implementation premise.

TWIC Milestones to Date

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

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

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

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

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

- The Coast Guard worked effectively with National Maritime Security Advisory Committee (NMSAC) to define secure areas. This definition will have a direct impact on over 10,000 vessels and more than 3,200 facilities. These secure areas delineate where a TWIC will be required for unescorted access.
- The joint rulemaking process between the Coast Guard and TSA was accelerated resulting in TWIC Notice of Proposed Rulemaking (NPRM) being published on May 22, 2006.
- The Coast Guard and TSA worked with industry partners to develop an interim process that compares a worker's biographical information against our terrorist watch lists and immigration databases.
- Facility owners, facility operators and unions submitted worker names, date of birth, and, as appropriate, alien identification number. The worker's immigration status was checked by the U.S. Citizenship and Immigration Service using its Central Index.
- To date TSA has completed 740,000 name-based threat assessments on port workers and longshoreman. These assessments were an interim measure and did not include the criminal history records check or biometric credential that is part of TWIC.

TWIC Rule and Stakeholder Input

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

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

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

- Creating a new process where TSA can make a determination that a security threat assessment conducted by another government agency is comparable, eliminating redundancy and reducing costs for workers;
- Providing workers more time to apply for an appeal or waiver;

- Streamlining the process, jointly with the Coast Guard, for merchant mariner credentialing and ensuring that there was no duplication of requirements resulting from the TWIC process.

TWIC cards will be required not only for port facility workers, but for anyone who seeks unescorted access to secure areas of a MTSA regulated facility or vessel, regardless of frequency. The workers covered by this rule include certain truck drivers, rail employees, security guards, longshoremen, as well as all U.S. merchant mariners. TSA will use the time tested security assessment procedures and standards that are currently used for commercial motor vehicle drivers licensed to transport hazardous materials, known as Hazardous Material Endorsements (HME). In short, TWIC will be issued to workers who successfully complete a security threat assessment, which includes: (1) a check against terrorist watch lists, (2) an immigration status check, and (3) a FBI fingerprint-based criminal history records check.

TWIC Card Readers

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

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

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

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

Rollout Contract

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

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

TWIC Card Costs

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

The fees for a TWIC will be slightly lower than was anticipated in the Final Rule. A TWIC will be $137.25 for a card that is valid for 5 years. Workers with current, comparable background checks (*e.g.,* HAZMAT, Merchant Mariner Document (MMD) or Free and Secure Trade (FAST)) will receive a discounted fee of $105.25. The cost of a lost, damaged or stolen credential is $36, although we have solicited comment on raising that fee.

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

Rollout Communication Plan and Pre-Enrollment

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

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

Enrollment Centers

Enrollment sites will be operated by trusted agents who are employees of a vendor under contract with TSA. These trained agents will have undergone a TSA security threat assessment before being allowed to collect the data. The trusted agents will provide applicants with a privacy notice and consent form, by which the applicant agrees to provide personal information for the security threat assessment and credential. The trusted agents will verify an applicant's identity, confirm the accuracy of biographic information, collect biometric information (a full set of fingerprints and a facial photograph), and obtain the applicant's signature on the enrollment documents. The contract performance parameter for the trusted advisor enroll-

ment process will be an average enrollment time of 15 minutes. The enrollment process for a pre-enrolled applicant is fully expected to take less time. As you can see, focused planning that fosters convenience for applicants will benefit workers as well as our process efficiencies.

Data Security Vetting and Card Issuance

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

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

Worker Redress/Waivers/Appeals

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

The standards for denial of a TWIC are the same standards that apply in the HME process. Any applicant who is subject to removal proceedings or an order of removal under the immigration laws of the United States is not eligible to apply for a TWIC. An individual will be disqualified if he or she lacks legal presence and/or authorization to work in the United States, has a connection to terrorist activity, or has been determined to lack mental capacity.

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

Individuals are ineligible for a TWIC if convicted in the last 7 years or incarcerated within the last 5 years of the following crimes: Unlawful possession, use or sale of a firearm or other weapon, extortion, fraud, bribery, smuggling, immigration violations, distribution or importation of a controlled substance, arson, kidnapping or hostage taking, rape or aggravated sexual abuse, assault with intent to kill, robbery, RICO violations that do not involve a permanent disqualifying crime.

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

Fairness and accuracy in TWIC waiver determinations are further ensured by an opportunity for independent review by an Administrative Law Judge. As previously

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

Lessons Learned and Future Efforts

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

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

- *Look for efficiencies in duplicative regulatory processes.* As noted previously, TSA and Coast Guard are developing procedures for the sharing of mariner fingerprints, identity verification, criminal history, and photographs for TWIC which is expected to save not only money but time. In addition, merchant mariners will no longer be required to visit a Regional Exam Center to obtain and renew their credentials, resulting in substantial time and travel savings.
- *Address the impact on small businesses.* TSA and the Coast Guard worked closely with the Small Business Administration to minimize the financial and operational impact on small businesses wherever possible. The rule includes provisions that allow MTSA-regulated passenger vessels (excluding cruise ships) to establish employee access areas for crewmembers that do not require unescorted access to secure areas such as the pilot house and engine room. This provision reduces the impact on those employees who rarely need to use spaces beyond those designated for support of passengers while maintaining the integrity of vessels' secure areas. We are also producing and distributing a Small Business Compliance Guide to assist small businesses in their implementation of the program.
- *When practicable, preserve state regulatory flexibility.* Mariner regulations and port security plans preempt state regulations. However, TSA does not preempt states from requiring background checks and badging systems in addition to TWIC. States may need to set standards for important purposes other than terrorism threats, such as preventing drug trafficking or organized crime.
- *Plan for privacy.* All data collected at an enrollment center will be deleted from the enrollment center work stations. The entire enrollment record (including all fingerprints collected) is stored in the TSA system, which is protected through role-based entry, encryption, and segmentation to prevent unauthorized use.
- *Technical innovation requires adaptive contract management.* TWIC is attempting to develop a 21st century technology that accommodates evolving IT standards suited to emergent needs that span local, international, public, and private interests. This requires continual reevaluation of the scope and methods of contracting. The recent Lockheed Martin contract award is a culmination of our efforts to date. Due to the nature of this task, however, we will need to continue to look for and implement adaptive planning, metrics, and changes to ensure this effort stays on track.
- *Don't expect a "silver bullet" technology solution.* Evolving technology, such as card readers, creates a changing environment and program control constraints. This is especially the case when the technology must be deployed to a vast multitude of entities with remote connectivity challenges (*e.g.,* vessels) and varying degrees of access control system capabilities.
- *Place the highest value in stakeholder input; it is time well spent.* The public hearings, comments to the NPRM, meetings with operators and associations, and contributions of advisory councils all added pure value. We came away from each and every one of these efforts better informed about the challenges, the unacceptable impacts, and the practicable options for protecting our ports.

Conclusion

The steps we are taking will be an extremely important aspect to the security of our port facilities and vessels. It's an effort which, when completed, will assure our citizens that those people who have unescorted access to secure areas of these port

facilities and vessels have been screened to make sure that they are not a security threat.

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

The CHAIRMAN. Thank you very much, sir.

And now I'll recognize Admiral Salerno.

STATEMENT OF BRIAN SALERNO, REAR ADMIRAL AND DIRECTOR OF INSPECTIONS AND COMPLIANCE, USCG, DHS

Admiral SALERNO. Good morning, Mr. Chairman and members of the Committee. Thank you for this opportunity to speak with you about the current status, and the way ahead for the TWIC Program.

I would specifically like to update the Committee on the Coast Guard's efforts, working in partnership with TSA to implement this program, which will strengthen maritime security, while balancing the need to facilitate commerce, and minimize negative effects on our port and vessel stakeholders.

Although the TWIC Program has not moved as rapidly as all of us would like, important milestones have been accomplished. Working relationships have been strengthened with the public and key industry stakeholders, and our commitment to protecting the maritime transportation system, while facilitating commerce, has not wavered.

Since publication of the final rule on January 25 of this year, the Coast Guard and TSA have continued to meet with our stakeholders in various venues. We've received considerable input on their ongoing concerns. These venues include the Passenger Vessel Association Conference, SMART card, and biometric industry conferences, maritime union meetings, and National Petro-Chemical Refiner's Association meeting, an American Waterways Operator's Executive Committee meeting, and the American Association of Port Authorities Conference, to name just a few.

The concerns expressed in these meetings have included the roll-out process for the initial TWIC cards, and the need to ensure that new hire provisions contained in the rules function as intended, which is of particular interest to small businesses. And, of course, the pilot program, which will pave the way for follow-on rulemaking for the card readers.

To address the roll-out, Coast Guard and TSA have worked together to develop supplemental documents, designed to assist those affected by the regulations. These documents include a Navigation and Vessel Inspection Circular, or NVIC, which is meant to explain the processes and procedures related to the implementation of the TWIC.

We have solicited and received input from the affected industry, as well as from Coast Guard field personnel on the draft of this NVIC, and have had generally positive feedback on the guidance contained within it.

We have also assisted in the development of two Small Business Administration compliance guides, and we have developed flyers, working with the contractor, Lockheed Martin, which will provide information to TWIC applicants.

We are also developing internal guidance documents for training, implementation and consistent enforcement. These documents will be cleared through Coast Guard Headquarters, and will be reviewed both by DHS and OMB, prior to distribution.

As we move into the implementation phase, we will continue working with industry to bring about the smooth transition to this much-needed security measure. We remain mindful of industry's concerns that vital provisions, such as the new-hire provision, function as intended, and our draft guidance reflects those concerns.

We also plan to verify that the security enhancement envisioned by the TWIC Program is having the intended effect. To this end, we intend to procure hand-held readers for use during our vessel and facility examinations and spot-checks.

After the compliance state is reached in a given port, the Coast Guard will use portable card readers to randomly check the validity of an individual's TWIC. This will serve as an interim measure, until the second rulemaking on card readers is finalized and put into effect.

Meanwhile, we are working very closely with DHS and TSA in coordinating the pilot program, which will provide key information and practical lessons learned to inform the second rulemaking. We requested, and received, recommendations from the National Maritime Security Advisory Committee, NMSAC, on technical specifications to be considered for card readers, which will be the subject of the second rulemaking. NMSAC's recommendations were also published in the *Federal Register* for public comment, and we are considering those comments carefully, to balance privacy, security and commerce, as we move forward with the card reader requirements.

TSA and Coast Guard continue to reach out to our private sector stakeholders, in the interest of fashioning regulations that will strengthen America's maritime security, while advancing commerce. While a TWIC Program is multi-faceted and includes numerous players, we are committed to developing a useful and valuable system.

Thank you for the opportunity to speak to you today, and I will be happy to take your questions.

[The prepared statement of Rear Admiral Salerno follows:]

PREPARED STATEMENT OF BRIAN SALERNO, REAR ADMIRAL AND DIRECTOR OF INSPECTIONS AND COMPLIANCE, USCG, DHS

Good morning, Senator Inouye, Senator Stevens, and members of the Committee. Thank you for this opportunity to speak with you about the current status and the way ahead for the Transportation Worker Identification Credential (TWIC) program. Specifically, I would like to update the Committee on the Coast Guard's efforts, in partnership with the Transportation Security Administration (TSA), to implement a program that will strengthen maritime security while balancing the need to facilitate commerce and minimize negative impacts to our port and vessel stakeholders.

Background and Authority

As a result of the Maritime Transportation Security Act (MTSA), the Coast Guard developed regulations establishing security requirements for maritime vessels and facilities posing a high risk of being involved in a transportation security incident. As part of these regulations, these vessels and facilities were required to conduct detailed security assessments and in turn, develop security plans under which owners and operators have been required to operate since July 1, 2004. The Coast Guard has been responsible for implementing and ensuring compliance with MTSA.

This same law requires the Department of Homeland Security (DHS) to issue a biometric transportation security card in order to be granted unescorted access to secure areas of vessels and facilities to those individuals who satisfactorily pass a security threat assessment. TSA was assigned this requirement, and because of our overlapping responsibilities, the Coast Guard and TSA formally joined efforts to carry out the TWIC program in November 2004. In this partnership, TSA is responsible for TWIC enrollment, security threat assessment and adjudication, card production, TWIC issuance, conduct of the TWIC appeal and waiver process, and management of government support systems. The Coast Guard is responsible for establishing and enforcing TWIC access control requirements at regulated vessels and facilities. Both agencies work very closely every day to make sure that our efforts achieve the objective of increased security that MTSA intended.

The TSA and the Coast Guard published a joint TWIC Notice of Proposed Rule Making (NPRM) on May 22, 2006. Following the publication of the NPRM and the subsequent comment period, Congress enacted the Security and Accountability for Every (SAFE) Port Act of 2006. The SAFE Port Act placed new statutory requirements for the TWIC Program. Among these requirements were: the commencement of a pilot program to test the viability of TWIC cards and readers in the maritime environment; deployment of the program in priority ports by set deadlines; inclusion of a provision to allow newly hired employees to work while the TWIC application was being processed; and concurrent processing of the TWIC and merchant mariner applications.

TSA and the Coast Guard published the TWIC final rule on January 25, 2007 in which the Coast Guard's MTSA regulations and TSA's Hazardous Material Endorsement regulations were amended to incorporate the TWIC requirements. This final rule did not require the installation of card readers at vessels and facilities as originally proposed in the NPRM. This requirement will be proposed during a second notice and comment rulemaking.

Joint Rulemaking by TSA and the USCG

In the TWIC Program, TSA is responsible for TWIC enrollment and issuance, including hardware and software applications and the data storage system. This responsibility involves conducting a security threat assessment on TWIC applicants, which includes a check against terrorist watch lists, an immigration status check, and a fingerprint-based criminal history records check, as well as perpetual vetting against the terrorist watch lists throughout the 5 year life of the TWIC. The Coast Guard is responsible for implementing TWIC in the maritime environment. The Coast Guard is achieving this by requiring a TWIC for all individuals who need unescorted access to secure areas of MTSA-regulated facilities and vessels and requiring a TWIC for all U.S. merchant mariners with active credentials.

TSA and the Coast Guard are also working together to develop several supplementary documents to help those affected by this regulation. These documents include a Navigation and Vessel Inspection Circular (NVIC); two Small Business Administration Compliance Guides; fliers for TWIC applicants; and internal guidance documents for training, implementation, and enforcement for Coast Guard and TSA personnel. Since publication of the Final Rule, the Coast Guard and TSA have conducted outreach at national venues such as the Passenger Vessel Association Conference; SMART card and biometric industry conferences; maritime union meetings; American Waterway Operators Executive Committee meeting; and the American Association of Port Authorities Conference to name a few.

Public Comments and Concerns

TSA and the Coast Guard received almost 2,000 comments on the TWIC NPRM. A general theme throughout the comments was the technological and economic feasibility of the TWIC cards and card readers in the maritime environment. While smart cards, open slot card readers, and the use of biometrics have been used for a number of years in controlled, office-like environments, very few studies have examined how currently approved biometric card readers will withstand the comparatively harsh environments of vessels and maritime facilities. Also, several commenters stated that the cost of biometric card readers would be extremely detrimental for small entities. TSA and the Coast Guard found the comments received to be invaluable in determining the best way forward for this rule.

Throughout February and March of this year, the Coast Guard also solicited comments from field units and industry stakeholders while drafting the TWIC Navigation and Vessel Inspection Circular. We received over 400 comments, which were used to construct a clear and thorough guidance document for industry and Coast Guard units during implementation. This guidance document is currently in concur-

rent clearance at Coast Guard Headquarters and will be reviewed by both DHS and OMB prior to distribution.

Pilot Program

Based on the comments received from all sources, the Department chose to bifurcate the rule. In order to address concerns about the adequacy of current reader technology, the Coast Guard is not requiring facility and vessel owner operators to purchase, install, and maintain card readers. We will address this requirement in a separate rulemaking following the pilot program required by the SAFE Port Act and will provide all interested parties ample opportunity to comment on the new proposals during the comment period following the second NPRM.

In addition, the National Maritime Security Advisory Committee (NMSAC) formed a working group of maritime industry and biometric technology representatives to propose specifications for TWIC cards and card readers using a contactless (or proximity) interface. The specifications were presented and approved on February 28, 2007 at NMSAC's quarterly meeting. A notice of availability of the specifications was published in the *Federal Register* for public comment on March 16, 2007. NMSAC's specifications will inform the pilot program set to begin in the Ports of Los Angeles/Long Beach, CA, in June 2007.

The Way Ahead

Work continues on several aspects of the TWIC Program. The Coast Guard is in the process of procuring handheld open slot card readers for use during vessel and facility inspections and spot checks. The Coast Guard will use the card readers to randomly check the validity of an individual's TWIC. Also, the provision for newly hired employees to work while they await issuance of a TWIC is in development and on track between the Coast Guard's Homeport web-portal engineers and TSA's Identity Data Management System engineers. Internally, policy is being written for implementation and enforcement of the TWIC Program in our ports through collaboration of our law enforcement, port security, and technology experts. We are working to meet the deadlines set by the SAFE Port Act.

Conclusion

TSA and the USCG continue to reach out to our private sector stakeholders in the interest of fashioning a regulation that strengthens America's maritime security while advancing commerce. While the TWIC Program is multifaceted and includes numerous players, we are committed to developing a useful and valuable system. I would be happy to take any questions you have at this time.

The CHAIRMAN. Thank you very much, Admiral.

May I now call upon Mr. Rabkin?

STATEMENT OF NORMAN J. RABKIN, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GAO

Mr. RABKIN. Chairman Inouye, members of the Committee, thank you very much for inviting me this morning to participate in this hearing on the status of the TWIC Program.

In December 2004, and September 2006, we reported on the status of the development and testing of the program. Our 2004 report identified challenges that TSA faced in developing regulations and a comprehensive plan for managing the TWIC Program, and several factors that caused TSA to miss the initial deadlines for issuing TWIC cards.

Our 2006 report identified the challenges encountered during the TWIC program testing, and several problems related to TWIC contract planning and oversight.

My testimony today focuses on two key areas, first, the progress that TSA has made since September, and second, some of the remaining challenges that TSA, the Coast Guard and the maritime industry must overcome to ensure the successful implementation of the TWIC Program.

TSA has made progress towards implementing TWIC and addressing several of the problems that we have previously identified regarding contract oversight, planning and coordination with stakeholders. Specifically, TSA has first issued the rule about enrolling workers and issuing the cards to workers in the maritime sector. Second, it has awarded a $70 million contract for enrolling these workers in the TWIC program. Third, it has assured us that it has a schedule for enrolling these workers and issuing the TWIC cards at ports, and conducting the pilot program to test TWIC access control technologies. Fourth, it has added staff with program and contract management expertise to help oversee the TWIC enrollment contract. And, finally, it has improved communications in coordination with the maritime stakeholders, and has plans for conducting public outreach and education efforts.

Nevertheless, TSA and the maritime industry stakeholders still face several challenges to ensuring that the TWIC Program can be implemented successfully. First, TSA and its enrollment contractor need to transition from limited testing of the TWIC Program, to successful implementation of the program on a much larger scale, covering over 770,000 workers at over 3,000–3,500 maritime facilities and over 5,000 vessels.

During testing, TSA issued TWIC cards to only about 1,700 workers, far short of its goal at that time of 75,000. Although TSA has learned from the testing experience, and has taken steps to help address problems that we previously identified, it remains to be seen whether TSA and the enrollment contractor will be able to implement the TWIC Program on such a large scale, in reasonable time-frames.

Second, TSA and the enrollment contractor will also need to educate workers about the TWIC requirements, ensure that enrollments begin in a timely manner, and process numerous background checks, appeals and waivers. Identifying the thousands of workers located throughout this and neighboring countries who will need to have the TWIC card, and educating them about their responsibilities for obtaining the card, will require a communication and coordination effort on the part of TSA and the enrollment contractor. Furthermore, processing these appeals, and doing so in a timely manner will also be a challenge.

Finally, TSA and the stakeholders must also ensure that the TWIC access control technologies will work effectively in the maritime environment, be compatible with the cards that have been issued, and will balance security with the flow of commerce. Access control technologies will need to withstand the harsh rigors of the maritime environment. If biometric card readers do not work effectively, ports could experience long lines, delaying other workers or trucks from entering. Such delays, of course, will negatively impact maritime commerce, costing port facilities time and money.

As TSA continues to implement the TWIC Program, we believe it should establish reasonable time-frames for holding itself, and its contractor accountable, and ensure that it learns and implements lessons as it phases in the enrollment function and pilot tests the access control technologies.

Mr. Chairman, this concludes my statement, and I also would be glad to answer your questions.

[The prepared statement of Mr. Rabkin follows:]

PREPARED STATEMENT OF NORMAN J. RABKIN, MANAGING DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GAO

Mr. Chairman and members of the Committee:

Thank you for inviting me to participate in today's hearing on the status of the Transportation Security Administration's (TSA) Transportation Worker Identification Credential (TWIC) program. Ensuring that only workers that do not pose a terrorist threat are allowed access to secure areas of the Nation's transportation facilities is critical to helping prevent a terrorist attack. The TWIC program was created to help protect these facilities from the threat of terrorism by issuing identification cards only to workers who do not pose a terrorist threat and allow these workers unescorted access to secure areas of the transportation system. To accomplish this objective, the TWIC program will include collection of personal and biometric information to validate workers' identities, background checks on transportation workers to ensure they do not pose a threat to security, issuance of tamper-resistant biometric credentials that cannot be counterfeited, verification of these credentials using biometric access control systems before a worker is granted unescorted access to a secure area, and revocation of credentials if disqualifying information is discovered, or if a card is lost, damaged, or stolen. The TWIC program was initially intended to serve all modes of transportation; however, TSA, in partnership with the Coast Guard, is focusing initial implementation on the maritime sector and is planning to implement the program in other modes in the future.

In December 2004 and September 2006, we reported on the status of the development and testing of the TWIC program.[1] Our 2004 report identified the challenges TSA faced in developing regulations and a comprehensive plan for managing the TWIC program and several factors that caused TSA to miss initial deadlines for issuing TWIC cards. Our September 2006 report identified the challenges encountered during TWIC program testing and several problems related to TWIC contract planning and oversight. In August 2006, TSA decided that the TWIC program would be implemented in the maritime sector using two separate rules. TSA issued the first rule in January 2007 requiring worker enrollment and card issuance and plans to issue a proposed rule on access control technologies in 2008. Since our September 2006 report, the Congress passed the Security and Accountability for Every (SAFE) Port Act of 2006, directing TSA, among other things, to implement the TWIC program at the 10 highest risk ports by July 1, 2007.[2] In January 2007, TSA awarded a $70 million contract to begin enrolling workers and issuing TWIC cards to workers at these maritime facilities.

My testimony today focuses on two key areas: (1) the progress TSA has made since September 2006 in implementing the TWIC program; and (2) some of the remaining challenges that TSA and the maritime industry must overcome to ensure the successful implementation of the TWIC program. My comments are based primarily on our December 2004 and September 2006 reports on the TWIC program, which reflect work conducted at TSA and the Coast Guard, as well as site visits to transportation facilities that participated in testing the TWIC program. In addition, in March and April 2007, we interviewed TSA officials and obtained some supporting documentation regarding the agency's efforts to implement the TWIC program. We also interviewed officials at port facilities in California, Delaware, and Florida that participated in TWIC testing concerning the implementation of the TWIC program. We conducted our work in accordance with generally accepted government auditing standards.

Summary

Since we issued our report on the TWIC program in September 2006, TSA has made progress toward implementing the TWIC program and addressing several of the problems that we previously identified regarding contract oversight and planning and coordination with stakeholders. Specifically, TSA has:

- issued a TWIC rule that sets forth the requirements for enrolling workers and issuing TWIC cards to workers in the maritime sector;
- awarded a $70 million contract for enrolling workers in the TWIC program,

[1] GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* GAO–05–106 (Washington, D.C.: December 2004), and *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO–06–982 (Washington, D.C.: September 2006).

[2] Pub. L. 109–347, 120 Stat. 1884, 1889 (2006).

- established a schedule for enrolling workers and issuing TWIC cards at ports and conducting a pilot program to test TWIC access control technologies,
- added staff with program and contract management expertise to help oversee the TWIC enrollment contract, and
- developed plans to improve communication and coordination with maritime stakeholders, including plans for conducting public outreach and education efforts.

TSA and maritime industry stakeholders still face several challenges to ensuring that the TWIC program can be implemented successfully:

- TSA and its enrollment contractor need to transition from limited testing of the TWIC program to successful implementation of the program on a much larger scale covering 770,000 workers at about 3,500 maritime facilities and 5,300 vessels.[3]
- TSA and its enrollment contractor will need to educate workers on the new TWIC requirements, ensure that enrollments begin in a timely manner, and process numerous background checks, appeals, and waivers.
- TSA and industry stakeholders will need to ensure that TWIC access control technologies will work effectively in the maritime environment, be compatible with TWIC cards that will be issued, and balance security with the flow of maritime commerce.

As TSA works to implement the TWIC program and begin enrolling workers, it will be important that the agency establish clear and reasonable time-frames and ensure that all aspects of the TWIC program, including the TWIC access control technologies, are fully tested in the maritime environment.

Background

Securing transportation systems and facilities is complicated, requiring balancing security to address potential threats while facilitating the flow of people and goods. These systems and facilities are critical components of the U.S. economy and are necessary for supplying goods throughout the country and supporting international commerce. U.S. transportation systems and facilities move over 30 million tons of freight and provide approximately 1.1 billion passenger trips each day. The Ports of Los Angeles and Long Beach estimate that they alone handle about 43 percent of the Nation's oceangoing cargo. The importance of these systems and facilities also makes them attractive targets to terrorists. These systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas. A terrorist attack at these systems and facilities could cause a tremendous loss of life and disruption to our society. An attack would also be costly. According to testimony by a Port of Los Angeles official, a 2002 labor dispute led to a 10-day shutdown of West Coast port operations, costing the Nation's economy an estimated $1.5 billion per day.[4] A terrorist attack to a port facility could have a similar or greater impact.

One potential security threat stems from those individuals who work in secure areas of the Nation's transportation system, including seaports, airports, railroad terminals, mass transit stations, and other transportation facilities. It is estimated that about 6 million workers, including longshoreman, mechanics, aviation and railroad employees, truck drivers, and others access secure areas of the Nation's estimated 4,000 transportation facilities each day while performing their jobs. Some of these workers, such as truck drivers, regularly access secure areas at multiple transportation facilities. Ensuring that only workers that do not pose a terrorism security risk are allowed unescorted access to secure areas is important in helping to prevent an attack. According to TSA and transportation industry stakeholders, many individuals that work in secure areas are currently not required to undergo a background check or a stringent identification process in order to access secure areas. In addition, without a standard credential that is recognized across modes of transportation and facilities, many workers must obtain multiple credentials to access each transportation facility they enter.

---

[3] TSA estimated the total number of workers, facilities, and vessels affected by the TWIC rule in the Regulatory Impact Assessment of the TWIC rule.

[4] Testimony of the Director of Homeland Security, Port of Los Angeles, before the U.S. Senate Committee on Commerce, Science, and Transportation, May 16, 2006.

TWIC Program History

In the aftermath of the September 11, 2001, terrorist attacks, the Aviation and Transportation Security Act (ATSA) was enacted in November 2001.[5] Among other things, ATSA required TSA to work with airport operators to strengthen access control points in secure areas and consider using biometric access control systems to verify the identity of individuals who seek to enter a secure airport area. In response to ATSA, TSA established the TWIC program in December 2001 to mitigate the threat of terrorists and other unauthorized persons from accessing secure areas of the entire transportation network, by creating a common identification credential that could be used by workers in all modes of transportation.[6] In November 2002, the Maritime Transportation Security Act of 2002 (MTSA) was enacted and required the Secretary of Homeland Security to issue a maritime worker identification card that uses biometrics, such as fingerprints, to control access to secure areas of seaports and vessels, among other things.[7]

The responsibility for securing the Nation's transportation system and facilities is shared by Federal, state, and local governments, as well as the private sector. At the Federal Government level, TSA, the agency responsible for the security of all modes of transportation, has taken the lead in developing the TWIC program, while the Coast Guard is responsible for developing maritime security regulations and ensuring that maritime facilities and vessels are in compliance with these regulations. As a result, TSA and the Coast Guard are working together to implement TWIC in the maritime sector. Most seaports, airports, mass transit stations, and other transportation systems and facilities in the United States are owned and operated by state and local government authorities and private companies. As a result, certain components of the TWIC program, such as installing card readers, will be the responsibility of these state and local governments and private industry stakeholders.

TSA—through a private contractor—tested the TWIC program from August 2004 to June 2005 at 28 transportation facilities around the Nation, including 22 port facilities, 2 airports, 1 rail facility, 1 maritime exchange, 1 truck stop, and a U.S. postal service facility. In August 2005, TSA and the testing contractor completed a report summarizing the results of the TWIC testing. TSA also hired an independent contractor to assess the performance of the TWIC testing contractor. Specifically, the independent contractor conducted its assessment from March 2005 to January 2006, and evaluated whether the testing contractor met the requirements of the testing contract. The independent contractor issued its final report on January 25, 2006.

Since its creation, the TWIC program has received about $79 million in funding for program development. (See *Table 1.*)

Table 1.—TWIC Program Funding From Fiscal Years 2002 to 2007

[Dollars in millions]

Fiscal Year	Appropriated	Reprogramming	Adjustments	Total funding
2002	0	0	0	0
2003	5.0	0	0	5.0
2004	49.7	0	0	49.7
2005	5.0	0	0	5.0
2006	0	15.0	0	15.0
2007	0	0	4.7	4.7
Total	59.7	15.0	4.7	79.4

Source: TSA.

Note: TSA's Fiscal Year 2008 Congressional justification includes $26.5 million in authority to collect fees from transportation workers for TWIC cards.

Key Components of the TWIC Program

The TWIC program is designed to enhance security using several key components (see *Fig. 1*). These include:

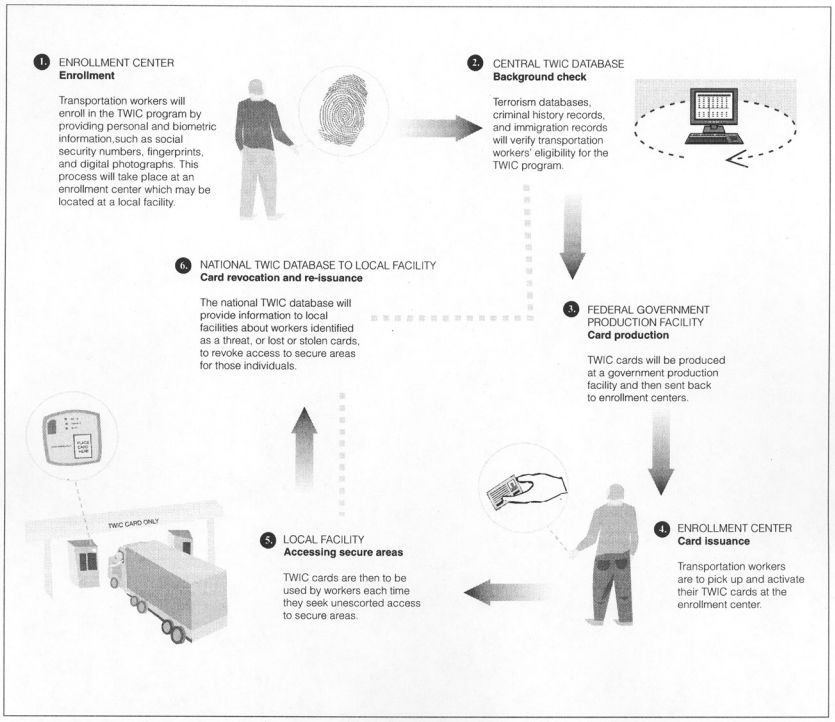
[5] Pub. L. 107–71, 115 Stat. 597 (2001).

[6] TSA was transferred from the Department of Transportation to the Department of Homeland Security pursuant to requirements in the Homeland Security Act of 2002 (Pub. L. 107–296, 116 Stat. 2135 (2002).

[7] Pub. L. 107–295, 116 Stat. 2064 (2002).

- *Enrollment*: Transportation workers will be enrolled in the TWIC program at enrollment centers by providing personal information, such as a social security number and address, and be photographed and fingerprinted. For those workers who are unable to provide quality fingerprints, TSA is to collect an alternate authentication identifier.
- *Background checks*: TSA will conduct background checks on each worker to ensure that individuals do not pose a security threat. These will include several components. First, TSA will conduct a security threat assessment that may include, for example, terrorism databases or terrorism watch lists, such as TSA's No-fly and selectee lists. Second, a Federal Bureau of Investigation criminal history records check will be conducted to identify if the worker has any disqualifying criminal offenses. Third, workers' immigration status and mental capacity will be checked. Workers will have the opportunity to appeal the results of the threat assessment or request a waiver in certain limited circumstances.
- *TWIC card production*: After TSA determines that a worker has passed the background check, the worker's information is provided to a Federal card production facility where the TWIC card will be personalized for the worker, manufactured, and then sent back to the enrollment center.
- *Card issuance*: Transportation workers will be informed when their cards are ready to be picked up at enrollment centers. Once a card has been issued, workers will present their TWIC cards to security officials when they seek to enter a secure area and in the future will enter secure areas through biometric card readers.

Figure 1: Overview of the TWIC process



Source: GAO analysis of TSA information.

TSA Has Made Progress Since September 2006 in Implementing the TWIC Program

Since we issued our report on the TWIC program in September 2006, TSA has made progress toward implementing the TWIC program and addressing several of the problems that we previously identified regarding contract oversight and planning and coordination with stakeholders. In January 2007, TSA and the Coast Guard issued a TWIC rule that sets forth the requirements for enrolling workers and issuing TWIC cards to workers in the maritime sector and awarded a $70 million contract for enrolling workers in the TWIC program. TSA is also taking steps designed to address requirements in the SAFE Port Act regarding the TWIC program, such as establishing a rollout schedule for enrolling workers and issuing TWIC cards at ports and conducting a pilot program to test TWIC access control technologies. TSA has also taken steps to strengthen TWIC contract planning and oversight and improve communication and coordination with its maritime stakeholders. Since September 2006, TSA reported that it has added staff with program and contract management expertise to help oversee the TWIC enrollment contract and taken additional steps to help ensure that contract requirements are met. In addition, TSA has also focused on improving communication and coordination with maritime stakeholders, such as developing plans for conducting public outreach and education efforts.

TSA Issued a TWIC Rule and Awarded a Contract To Begin Enrolling Workers and Issuing TWIC Cards This Year

On January 25, 2007, TSA and the Coast Guard issued a rule that sets forth the regulatory requirements for enrolling workers and issuing TWIC cards to workers in the maritime sector. Specifically, the TWIC rule provides that workers and merchant mariners requiring unescorted access to secure areas of maritime facilities and vessels must enroll in the TWIC program, undergo a background check, and obtain a TWIC card before such access is granted. In addition, the rule requires owners and operators of maritime facilities and vessels to change their existing access control procedures to ensure that merchant mariners and any other individual seeking unescorted access to a secure area of a facility or vessel has a TWIC. *Table 2* describes the specific requirements in the TWIC rule.

Table 2.—Requirements in the TWIC Rule

Requirement	Description of requirement
Transportation workers	Individuals who require unescorted access to secure areas of maritime facilities and vessels and all merchant mariners must obtain a TWIC card before such access is granted.
Fees	All workers applying for a TWIC card will pay a fee of $137 to cover the costs associated with the TWIC program. Workers that have already undergone a Federal threat assessment comparable to the one required to obtain a TWIC will pay a reduced fee of $105. The interim replacement fee for a TWIC card will be $36.
Access to secure areas of maritime facilities and vessels	By no later than September 25, 2008, facilities and vessels currently regulated by the Maritime Transportation Security Act must change their current access control procedures to ensure that any individual or merchant mariner seeking unescorted access to a secure area has a TWIC card.
Newly hired workers and escorting procedures	Newly hired workers, who have applied for, but have not received their TWIC card, will be allowed access to secure areas for 30 days as long as they meet specified criteria, such as passing a TSA name-based background check, and only while accompanied by another employee with a TWIC card. Individuals that need to enter a secure area but do not have a TWIC card must be escorted at all times by individuals with a TWIC card.
Background checks	All workers applying for a TWIC card must provide specific types of personal information and fingerprints to TSA to conduct a security threat assessment, that includes an FBI fingerprint-based criminal history records check, and an immigration status check. In order to receive a TWIC card, workers must not have been incarcerated or convicted of certain crimes within prescribed time periods, must have legal presence or authorization to work in the United States, have no connection to terrorist activity, and cannot have been found as lacking mental capacity or have been committed to a mental health facility.

Table 2.—Requirements in the TWIC Rule—Continued

Requirement	Description of requirement
Appeals and waiver process	All TWIC applicants will have the opportunity to appeal a background check disqualification through TSA or apply to TSA for a waiver, either during the application process, or after being disqualified for certain crimes, mental incapacity, or are aliens in Temporary Protected Status. Applicants who appeal or seek a waiver and are denied by TSA may seek review by an administrative law judge.
Access control systems	The Coast Guard will conduct unannounced checks to confirm the identity of TWIC card holders using hand-held biometric card readers to check the biometric on the TWIC card against the person presenting the card. In addition, security personnel will conduct visual inspections of the TWIC cards and look for signs of tampering or forgery when a worker enters a secure area.

Source: GAO analysis of TWIC rule.

The TWIC rule does not include the requirements for owners and operators of maritime facilities and vessels to purchase and install TWIC access control technologies, such as biometric TWIC card readers. As a result, the TWIC card will initially serve as a visual identity badge until access control technologies are required to verify the credentials when a worker enters a secure area. According to TSA, during the program's initial implementation, workers will present their TWIC cards to authorized security personnel, who will compare the cardholder to his or her photo and inspect the card for signs of tampering. In addition, the Coast Guard will verify TWIC cards when conducting vessel and facility inspections and during spot checks using hand-held biometric card readers to ensure that credentials are valid. According to TSA, the requirements for TWIC access control technologies will be set forth in a second proposed rule to be issued in 2008, at which time TSA will solicit public comments and hold public meetings.

As part of the TWIC rule, TSA is also taking steps designed to address various requirements of the SAFE Port Act including that it implement TWIC at the 10 highest risk ports by July 1, 2007. According to TSA, the agency has categorized ports based on risk and has developed a schedule for implementing TWIC at these ports to address the deadlines in the SAFE Port Act. In addition, TSA is currently planning to conduct a pilot program at five maritime locations to test TWIC access control technologies, such as biometric card readers, in the maritime environment. According to TSA, the agency is partnering with the Ports of Los Angeles and Long Beach to test TWIC access control technologies and plans to select additional ports to participate in the pilot in the near future. TSA and Port of Los Angeles officials told us that ports participating in the pilot will be responsible for paying for the costs of the pilot and plan to use Federal port security grant funds for this purpose. According to TSA, the agency plans to begin the pilot in conjunction with the issuance of TWIC cards so the access control technologies can be tested with the cards that are issued to workers. Once the pilot has been completed, TSA plans to use the results in developing its proposed rule on TWIC access control technologies.

Following the issuance of the TWIC rule in January 2007, TSA awarded a $70 million contract to a private company to enroll the estimated 770,000 workers required to obtain a TWIC card. According to TSA officials, the contract costs include $14 million for the operations and maintenance of the TWIC identity management system that contains information on workers enrolled in the TWIC program, $53 million for the cost of enrolling workers, and $3 million designated to award the enrollment contractor in the event of excellent performance. TSA officials stated that they are currently transitioning the TWIC systems to the enrollment contractor and testing these systems to ensure that they will function effectively during nationwide implementation. TSA originally planned to begin enrolling workers at the first port by March 26, 2007—the effective date of the TWIC rule. However, according to TSA officials, initial enrollments have been delayed. While TSA officials did not provide specific reasons for the delay, officials from the port where enrollments were to begin told us that software problems were the cause of the delay, and could postpone the first enrollments until May 2007. In addition, TSA and the Coast Guard have not set a date by which workers will be required to posses a TWIC card to access secure areas of maritime facilities and vessels. According to the TWIC rule, once the agency determines at which ports TWIC will be implemented and by what date, this schedule will be posted to the *Federal Register*.

TSA Has Taken Steps to Strengthen Contract Planning and Oversight and Better Coordinate With Maritime Industry Stakeholders

Since we issued our September 2006 report, TSA has taken several steps designed to strengthen contract planning and oversight. We previously reported that TSA experienced problems in planning for and overseeing the contract to test the TWIC program, which contributed to a doubling of TWIC testing contract costs and a failure to test all key components of the TWIC program. We recommended that TSA strengthen contract planning and oversight before awarding a contract to implement the TWIC program. TSA acknowledged these problems and has taken steps to address our recommendations. Specifically, TSA has taken the following steps designed to strengthen contract planning and oversight:

- Added staff with expertise in technology, acquisitions, and contract and program management to the TWIC program office.
- Established a TWIC program control office to help oversee contract deliverables and performance.
- Established monthly performance management reviews and periodic site visits to TWIC enrollment centers to verify performance data reported by the contractor.
- Required the enrollment contractor to survey customer satisfaction as part of contract performance.

In addition to these steps, TSA has established a TWIC quality assurance surveillance plan that is designed to allow TSA to track the enrollment contractor's performance in comparison to acceptable quality levels. This plan is designed to provide financial incentives for exceeding these quality levels and disincentives, or penalties, if they are not met. According to the plan, the contractor's performance will be measured against established milestones and performance metrics that the contractor must meet for customer satisfaction, enrollment time, number of failures to enroll, and TWIC help desk response times, among others. TSA plans to monitor the contractor's performance through monthly performance reviews and by verifying information on performance metrics provided by the contractor.

In addition to contract planning and oversight, TSA has also taken steps designed to address problems that were identified in our September 2006 report regarding communication and coordination with maritime stakeholders. We previously reported that stakeholders at all 15 TWIC testing locations that we visited cited poor communication and coordination by TSA during testing of the TWIC program. For example, TSA never provided the final results or report on TWIC testing to stakeholders that participated in the test, and some stakeholders stated that communication from TSA would stop for months at a time during testing. We recommended that TSA closely coordinate with maritime industry stakeholders and establish a communication and coordination plan to capture and address the concerns of stakeholders during implementation. TSA acknowledged that the agency could have better communicated with stakeholders at TWIC testing locations and has reported taking several steps to strengthen communication and coordination since September 2006. For example, TSA officials told us that the agency developed a TWIC communication strategy and plan that describes how the agency will communicate with the owners and operators of maritime facilities and vessels, TWIC applicants, unions, industry associations, Coast Guard Captains of the Port, and other interested parties. In addition, TSA required that the enrollment contractor establish a plan for communicating with stakeholders.

TSA, the Coast Guard, and the enrollment contractor have taken additional steps designed to ensure close coordination and communication with the maritime industry. These steps include:

- Posting frequently asked questions on the TSA and Coast Guard websites.
- Participating in maritime stakeholder conferences and briefings.
- Working with Coast Guard Captains of the Ports and the National Maritime Security Advisory Committee to communicate with local stakeholders.
- Conducting outreach with maritime facility operators and port authorities, including informational bulletins and fliers.
- Creating a TWIC stakeholder communication committee chaired by TSA, the Coast Guard, and enrollment contractor, with members from 15 maritime industry stakeholder groups. According to TSA, this committee will meet twice per month during the TWIC implementation.

Several stakeholders we recently spoke to confirmed that TSA and its enrollment contractor have placed a greater emphasis on communicating and coordinating with

stakeholders during implementation and on correcting past problems. For example, an official from the port where TWIC will first be implemented stated that, thus far, communication, coordination, and outreach by TSA and its enrollment contractor have been excellent, and far better than during TWIC testing. In addition, the TWIC enrollment contractor has hired a separate subcontractor to conduct a public outreach campaign to inform and educate the maritime industry and individuals that will be required to obtain a TWIC card about the program. For example, the port official stated that the subcontractor is developing a list of trucking companies that deliver to the port, so information on the TWIC enrollment requirements can be mailed to truck drivers.

TSA and Industry Stakeholders Need To Address Challenges To Ensure the TWIC Program Is Implemented Successfully

TSA and maritime industry stakeholders need to address several challenges to ensure that the TWIC program can be implemented successfully. As we reported in September 2006, TSA and its enrollment contractor face the challenge of transitioning from limited testing of the TWIC program to successful implementation of the program on a much larger scale covering 770,000 workers at about 3,500 maritime facilities and 5,300 vessels. Maritime stakeholders we spoke to identified additional challenges to implementing the TWIC program that warrant attention by TSA and its enrollment contractor, including educating workers on the new TWIC requirements, ensuring that enrollments begin in a timely manner, and processing numerous background checks, appeals, and waiver applications. Furthermore, TSA and industry stakeholders also face difficult challenges in ensuring that TWIC access control technologies will work effectively in the maritime environment, be compatible with TWIC cards that will be issued soon, and balance security with the flow of maritime commerce.

TSA and Its Contractor Face Challenges in Enrolling and Issuing TWIC Cards to Large Populations of Workers at Numerous Port Facilities and Vessels

In September of 2006, we reported that TSA faced the challenge of enrolling and issuing TWIC cards to a significantly larger population of workers in a timely manner than was done during testing of the TWIC program. In testing the TWIC program, TSA enrolled and issued TWIC cards to only about 1,700 workers at 19 facilities, well short of its goal of 75,000. According to TSA and the testing contractor, the lack of volunteers to enroll in the TWIC program testing and technical difficulties in enrolling workers, such as difficulty in obtaining workers' fingerprints to conduct background checks, led to fewer enrollments than expected. TSA reports that it used the testing experience to make improvements to the enrollment and card issuance process and has taken steps to address the challenges that we previously identified. For example, TSA officials stated that the agency will use a faster and easier method of collecting fingerprints than was used during testing and will enroll workers individually during implementation, as opposed to enrolling in large groups, as was done during testing. In addition, the TWIC enrollment contract Statement of Work requires the contractor to develop an enrollment test and evaluation program to ensure that enrollment systems function as required under the contract. Such a testing program will be valuable to ensure that these systems work effectively prior to full-scale implementation. We also reported that TSA faced the challenge of ensuring that workers are not providing false information and counterfeit identification documents when they enroll in the TWIC program. According to TSA, the TWIC enrollment process to be used during implementation will use document scanning and verification software to help determine if identification documents are fraudulent, and personnel responsible for enrolling workers will be trained to identify fraudulent documents.

Since we issued our report in September 2006, we have also identified additional challenges to implementing the TWIC program that warrant attention by TSA and its enrollment contractor. We recently spoke with some maritime stakeholders that participated in TWIC testing and that will be involved in the initial implementation of the program to discuss their views on the challenges of enrolling and issuing TWIC cards to workers. These stakeholders expressed concerns regarding the following issues:

Educating workers: TSA and its enrollment contractor face a challenge in identifying all workers that are required to obtain a TWIC card, educating them about how to enroll and receive a TWIC card, and ensuring that they enroll and receive a TWIC card by the deadlines to be established by TSA and the Coast Guard. For example, while longshoremen who work at a port every day may be aware of the new TWIC requirements, truck divers that deliver to the port may be located in different states or countries, and may not be aware of the requirements.

Timely enrollments: One stakeholder expressed concern about the challenges the enrollment contractor faces in enrolling workers at his port. For example, at this port, the enrollment contractor has not yet begun to lease space to install enrollment centers—which at this port could be a difficult and time-consuming task due to the shortage of space. Stakeholders we spoke to also suggested that until TSA establishes a deadline for when TWIC cards will be required at ports, workers will likely procrastinate in enrolling, which could make it difficult for the contractor to enroll large populations of workers in a timely manner.

Background checks: Some maritime organizations are concerned that many of their workers will be disqualified from receiving a TWIC card by the background check. These stakeholders emphasized the importance of TSA establishing a process to ensure timely appeals and waivers process for the potentially large population of workers that do not pass the check. According to TSA, the agency already has established processes for conducting background checks, appeals, and waivers for other background checks of transportation workers. In addition, TSA officials stated that the agency has established agreements with the Coast Guard to use their administrative law judges for appeal and waiver cases and plans to use these processes for the TWIC background check.

TSA and Industry Stakeholders Face Challenges in Ensuring That TWIC Access Control Technologies Work Effectively and Balancing Security With the Flow of Maritime Commerce

In our September 2006 report, we noted that TSA and maritime industry stakeholders faced significant challenges in ensuring that TWIC access control technologies, such as biometric card readers, worked effectively in the maritime sector. Few facilities that participated in TWIC testing used biometric card readers that will be required to read the TWIC cards in the future. As a result, TSA obtained limited information on the operational effectiveness of biometric card readers, particularly when individuals use these readers outdoors in the harsh maritime environment, where they can be affected by dirt, salt, wind, and rain. In addition, TSA did not test the use of biometric card readers on vessels, although they will be required on vessels in the future. Also, industry stakeholders we spoke to were concerned about the costs of implementing and operating TWIC access control systems, linking card readers to their local access control systems, connecting to TSA's national TWIC database to obtain updated security information on workers, and how biometric card readers would be implemented and used on vessels and how these vessels would communicate with TSA's national TWIC database remotely. Because of comments regarding TWIC access control technology challenges that TSA received from maritime industry stakeholders on the TWIC proposed rule, TSA decided to exclude all access control requirements from the TWIC rule issued in January 2007. Instead, TSA plans to issue a second proposed rule pertaining to access control requirements in 2008, which will allow more time for maritime stakeholders to comment on the technology requirements and TSA to address the challenges that we and stakeholders identified.

Our September 2006 report also highlighted the challenges that TSA and industry stakeholders face in balancing the security benefits of the TWIC program with the impact the program could have on maritime commerce. If implemented effectively, the security benefits of the TWIC program in preventing a terrorist attack could save lives and avoid a costly disruption in maritime commerce. Alternatively, if key components of the TWIC program, such as biometric card readers, do not work effectively, they could slow the daily flow of maritime commerce. For example, if workers or truck drivers have problems with their fingerprint verifications on biometric card readers, they could create long queues delaying other workers or trucks waiting in line to enter secure areas. Such delays could be very costly in terms of time and money to maritime facilities. Some stakeholders we spoke to also expressed concern with applying TWIC access control requirements to small facilities and vessels. For example, smaller vessels could have crews of less than 10 persons, and checking TWIC cards each time a person enters a secure area may not be necessary. TSA acknowledged the potential impact that the TWIC program could have on the flow of maritime commerce and plans to obtain additional public comments on this issue from industry stakeholders and develop solutions to these challenges in the second rulemaking on access control technologies.

In our September 2006 report, we recommended that TSA conduct additional testing to ensure that TWIC access control technologies work effectively and that the TWIC program balances the added security of the program with the impact that it could have on the flow of maritime commerce. As required by the SAFE Port Act, TSA plans to conduct a pilot program to test TWIC access control technologies in the maritime environment. According to TSA, the pilot will test the performance of

biometric card readers at various maritime facilities and on vessels as well as the impact that these access control systems have on facilities and vessel business operations. TSA plans to use the results of this pilot to develop the requirements and procedures for implementing and using TWIC access control technologies in the second rulemaking.

Conclusion

Preventing unauthorized persons from entering secure areas of the Nation's ports and other transportation facilities is critical to preventing a terrorist attack. The TWIC program was initiated in December 2001 to mitigate the threat of terrorists accessing secure areas. Since our September 2006 report, TSA has made progress toward implementing the program, including issuing a TWIC rule, taking steps to implement requirements of the SAFE Port Act, and awarding a contract to enroll workers in the program. While TSA plans to begin enrolling workers and issuing TWIC cards in the next few months, it is important that the agency establish clear and reasonable time-frames for implementing TWIC. TSA officials told us that the agency has taken steps to improve contract oversight and communication and coordination with its maritime TWIC stakeholders since September 2006. While the steps that TSA reports taking should help to address the contract planning and oversight problems that we have previously identified and recommendations we have made, the effectiveness of these steps will not be clear until implementation of the TWIC program begins. In addition, significant challenges remain in enrolling about 770,000 persons at about 3,500 facilities in the TWIC program. As a result, it is important that TSA and the enrollment contractor make communication and coordination a priority to ensure that all individuals and organizations affected by the TWIC program are aware of their responsibilities. Further, TSA and industry stakeholders need to address challenges regarding enrollment and TWIC access control technologies to ensure that the program is implemented effectively. It is important that TSA and the enrollment contractor develop a strategy to ensure that any potential problems that these challenges could cause are addressed during TWIC enrollment and card issuance. Finally, it will be critical that TSA ensure that the TWIC access control technology pilot program fully test all aspects of the TWIC program on a full scale in the maritime environment and the results be used to ensure a successful implementation of these technologies in the future.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have at this time.

Senator LAUTENBERG [presiding]. Thank you very much. Mr. Hawley, how many workers nationwide do you expect will need TWIC cards?

Mr. HAWLEY. The initial estimate is somewhere between 750,000 and 1.5 million.

Senator LAUTENBERG. That's a fairly broad spread. Well, the Port of New York and New Jersey currently issues some form of ID to allow access to port facilities, and they believe that they need 128,000 TWIC cardholders among the workers. And that's double what TSA's contractor has estimated. So, what figures does TSA intend to use? Because that's going to determine what resources need to be available to provide these cards in a timely and efficient manner.

Mr. HAWLEY. Yes, sir. I think it points out some of the improvements that have been made recently in the program, in that the contractor, in this case Lockheed Martin, is paid by the card. That's their incentive to do it quickly and well. It is scaleable and if we need to increase the number of cards, they're able to scale right along with that. And so, we do not have a situation where we have got a particular appropriation that we have to fit everything in. It is whatever the Coast Guard identifies as those positions, or the people who work in areas, that need this security. As many people that fall under that category, our contractor has the capacity to enroll.

Senator LAUTENBERG. But it has to be paid for.

Mr. HAWLEY. Yes. It's paid for by itself. In other words, when the port worker pays $137.25, that pays for the card and what's behind it.

Senator LAUTENBERG. Is it fair to ask the cardholders, the workers, to pay for, $137 in fee if the card readers are not going to be in place at the time? It's not fair to ask them to underwrite a development program.

Mr. HAWLEY. They're not underwriting the development. They're underwriting the cost of their card; and it's a professional credential that they have. It comes out to about $30 a year that it will cost them. So, it has less to do with the specific workplace, and everything to do about that individual. Because once an individual has a TWIC card, they have been verified. They can take it anywhere in the maritime sector. It will first, work, and second, meet all of the security requirements without question. So, it's an extraordinary value to the individuals who get them; and for $30 a year, that's a good deal.

Senator LAUTENBERG. Well, how about the value to the country? It seems unfair to me to ask them to pay for something that still has a long way to go in terms of development. How many card readers are there in place now?

Mr. HAWLEY. Well, those are done in the private sector, and the ones that will be specifically related to TWIC, we've put that off based on the stakeholders input, including all of the workers, of wanting to have a full opportunity to explore that, and have a notice and comment period before that is selected. So, the card is flexible enough to be compatible with the standards that are selected.

And, I think as Admiral Salerno mentioned, our Advisory Committee has come back with draft standards for that, that showed the way.

Senator LAUTENBERG. How is that cost determined, Mr. Hawley; to be sufficient to cover the cost of the card preparation. And if someone has a short-term job going into the port, are they going to have to pay $135 or $137? And depending upon the private sector, not fully, to have the card readers there, and they're not in place at this point.

Mr. HAWLEY. That's correct. But there is significant security value for the card. Just having the card, and as Admiral Salerno mentioned, the check-in. Maybe the Admiral could mention the new-hire process and the other security.

Senator LAUTENBERG. Wouldn't it, according to your policy, Admiral Salerno, only Coast Guard personnel can confiscate a misused TWIC card. Local law enforcement, and they are limited to holding an individual until Coast Guard personnel arrives to confiscate the TWIC card. That's a pretty cumbersome system. Wouldn't it make more sense to allow bona fide law enforcement officials to confiscate a TWIC card based on a reasonable cause?

Admiral SALERNO. Senator, the policy was put in place so that we could maintain control over the system. The facility operator has the authority to deny entry to any person that does not have reason to be on the facility, so we would anticipate——

Senator LAUTENBERG. Can they confiscate the card?

Admiral SALERNO. They would not confiscate the card, that would be done by Coast Guard personnel.

Senator LAUTENBERG. Well, if a card has been denied access, then that would obviously have to be proven, perhaps, in a court room. How efficient can the system be if they have to wait for Coast Guard to catch up with this person, and confiscate the card?

Admiral SALERNO. Senator, we do—as you know—have a presence in all of the major ports, and have teams of people who are tasked with conducting facility inspections, and vessel inspections, and it's a part of their job description that they would visit these facilities on a regular basis. So, by notifying the Coast Guard, these teams could be dispatched to take whatever action——

Senator LAUTENBERG. I think you're going to have to look very deeply into that problem, because it seems to me that the Coast Guard is busy altogether. I always think that the Coast Guard has been issued too many assignments for the body of personnel that it has. And when I think of them having to run down and confiscate the card.

And I think about an employer's dilemma—got a lot of work to do, I'm going to pick up these cards from these three fellows, and put them aside—would they only be people that were on they, who don't qualify to pass the terrorist watch list?

Admiral SALERNO. It would be, in cases where it appears to be held by a person who's not entitled to a card, some fraudulent activity. It would not be based on the background check itself, that would be done—we would not issue a card unless a person has passed the background check. It would only be in cases where there appears to be something inappropriate taking place.

Senator LAUTENBERG. Without these card readers in place, I think what we'll see is more confusion and longer delays.

Mr. Hawley, it's my understanding that TSA has suggested taking resources from the Port Security Grant Program to pay for the TWIC pilot project. Why wasn't funding requested separately for the pilot project?

Mr. HAWLEY. Well, the pilot project relates to access control, and that has to be the subject of—it will have pilots, and then the rulemaking. The standards are just now being set. And we have a number of ports who have come forward, including ports in New York, and New Jersey, who are anxious to be among the pilot. Since it is a permanent part of the port infrastructure that they're doing, it is eligible for the Port Security Grant. So, that is a way to jumpstart the program, and then as we work further to define the nature of the other pilots, that's when we'll look at the money and see if we need more, and if we do, we'll ask for it.

But, the Port Security Grants, that's what they're for, and this is a process that's already underway, and they can move very quickly to get them going.

Senator LAUTENBERG. Are you comfortable with the progress made thus far, and the ability to set a target date to get things relatively in place to effectively read the cards? What's the timeline that you suggest would be a timeline that could be met? And where we're really getting a test of this—I mean, issuing the cards is one part of it, but I think the larger part in terms of having it work

effectively is whether or not these can be read electronically, and with some degree of dispatch, get them done?

Mr. HAWLEY. Yes, I think the—one of the features of the standard that we'll have for the access control system is the flexibility to allow the individual operators to use their own existing access control. That can be enabled on the card. So the TWIC cards, when issued, will be able to be used immediately in that environment.

Senator LAUTENBERG. Well. We don't have to look through the list to——

Senator CARPER. It's just us.

Senator LAUTENBERG.—see who's next. Senator Carper?

STATEMENT OF HON. THOMAS R. CARPER, U.S. SENATOR FROM DELAWARE

Senator CARPER. Gentlemen, welcome. It's good to see you, Secretary Hawley, Admiral Salerno. I said to Beth Osborne, a member of my staff, "Is it my imagination, or are the Admirals getting younger?"

Mr. Rabkin, thank you for coming, and thanks for all of the good work that you do at GAO.

We have a special interest in this particular issue in Delaware because of the Port of Wilmington. Not everybody in the audience who might be watching this hearing knows that the Port of Wilmington is the top banana port, and we all want to be top banana in some respect or the other, and for us in Delaware, our port is a place where a lot of bananas come through. If you ate a banana this morning with your cereal, there's a pretty good chance that it came through the Port of Wilmington. We're a big port for Chilean fruit, all kinds of stuff that we bring through that helps feed—especially people on the eastern side of our country.

We bring in other things, and export among other things, the Saturn Sky. We don't export a lot of automobiles, but we export the Saturn Sky, made in Wilmington, Delaware by GM.

But, we're proud of our port, and it's a major employer, and not just at the port, but also helps support a variety of businesses and parts of our economy, not just in Delaware, but in the Greater Delaware Valley and the Del Mar Peninsula. So, we have more than a little bit of interest, as you might imagine.

This is an issue we've followed for a few years in Delaware, and Delaware was the first state to ratify the Constitution and our moniker is "The First State"—we like to be first in a whole lot of things.

I think we might get to be first with respect to the TWIC card. And, it has taken us awhile to get here, and one of the questions I wanted to ask, and one of the things I'd like to explore with the panel is a little bit of chronology. When was the first gleam in somebody's eye that there ought to be a TWIC card, and did it grow out of legislation in 2001, was it part of the Patriot Act, was there, was it part of the Maritime Transportation Security Act, is that where the genesis really lies?

Mr. HAWLEY. I believe out of MTSA was where TWIC was originated.

Senator CARPER. All right. Could somebody just kind of walk me through the TWIC in terms—I think, if someone had said back

when the legislation was enacted that we'd still be here, and, in the Spring of 2007, waiting to implement the program, in even one port, I think folks would have been surprised. We're told, the folks in Wilmington, the Port of Wilmington are told that we can anticipate the initial deployment maybe in May, and now we're hearing it may not be May, we were told before it was before May.

So, first question—somebody, I don't care, Mr. Rabkin, if it's you, I don't care, Secretary Hawley, if it's you—somebody just kind of walk us through why it has taken this long?

Mr. Hawley, you've not been in your job forever, I know that, I know that—how many years have you been there?

Mr. HAWLEY. About a year and a half.

Senator CARPER. How long does it seem?

[Laughter.]

Mr. HAWLEY. About that.

Senator CARPER. OK. You've not been there since this legislation—but why so long?

Mr. HAWLEY. Well, it has to do with the system that's behind the card. As you know, it is that network behind the card that is complex. We made some decisions in the last year, that added complexity, and therefore, probably time, to the process. But it was, in our view, worth it. It has to be compliant with the FIPS 201 process, which is the latest Federal Government biometrics standard. So changes were needed to align TWIC with that. We thought that was prudent going forward.

And then there were some privacy data issues, gaps identified by our internal folks as well as the DHS Inspector General. So, we had to get after those, and close those, and that's now done as of February. And the rulemaking, we went through a long rulemaking. We had 1,900 comments. So that's why, that's why it has taken so long.

Senator CARPER. Do you have, do you have a fair amount of confidence that we're almost—I'll use a football metaphor—the ball is almost in the end zone?

Mr. HAWLEY. Well, it—which end zone? No, but I think the——

[Laughter.]

Mr. HAWLEY. Yes, I do. I think a year ago, all of the points that Mr. Rabkin made and the Chairman made earlier in terms of where is your process; where are your professional program managers, a whole lot of those things have now been fixed. The system is built. We've awarded the procurement; and now we're in the stage of testing. The hard part about testing is you just don't know how long it's going to take, because if it passes the first try, we're out of here and ready to go. And because of the importance of it in the real world, we're not going to move forward until the testing is done. That is the reason why the cards are not being issued today, because the testing is not complete.

So, in answer to the Port of Wilmington, which will be first for TWIC and when I mentioned in my opening about the port community being enormously forthcoming and constructive, the Port of Wilmington leads that charge, and we will have a minimum of a 45-day head start before we begin to go to the port and start enrollment. So, whenever we get to that point, the TSA, the Coast Guard

will communicate with the port, and then there will be plenty of time to get the thing up and running.

Senator CARPER. Thank you.

Mr. Rabkin, should we be encouraged that we're making reasonable progress and the expectations that Secretary Hawley has suggested will be realized?

Mr. RABKIN. Well, I think there's reasonable progress, but I'm not as optimistic as the Secretary is about how much has been shown, and how close we are—if I may—to the goal line. TSA conducted a prototype test that was underwhelming, it did not achieve any of its goals, although it did create some lessons to be learned, and I think the TSA has learned those lessons.

They still have to meet certain deadlines, they have to hold their contractor accountable for getting this next test of issuing cards in the 10 highest-risk ports done, and it's not off to a very auspicious start, because it's delayed there, and we're still not confident about when it's even going to start, let alone finish.

And then, that's just getting the cards out. It's a very important process, but from my perspective, that's the easy part. And then they have to move the technology, and having it work, and work quickly and work accurately, all the time, is, I think, even more of a major challenge. So, there's a lot to be done yet.

Senator CARPER. Let me follow up with a question about communication; between TSA and whether it's the Port of Wilmington or other ports that will be coming down the road here. Just tell us about the quality of that communication, are you satisfied with it? Is it getting better? We've been told it has been—from our perspective, not very good.

Mr. HAWLEY. Well, I think the communication is excellent, actually. And, it's a team thing between the Coast Guard and TSA, and now our contractor. And we've stood up a formal consultative group to formalize that process.

Senator CARPER. I'm talking about communicating with ports, with the folks that are——

Mr. HAWLEY. Well, first of all, the Coast Guard is in the port.

Admiral SALERNO. If I may, sir——

Senator CARPER. Please.

Admiral SALERNO. In each port there is a, what we call an Area of Maritime Security Committee which represents a broad cross-section of stakeholders in the port. In addition, there is a harbor safety committee, which again, represents broad sections of the port. One is for security purposes, one for safety, but each of them represent opportunities to reach out and communicate with the full spectrum of port stakeholders.

We have communicated with our staffs in all of the ports, and have prepped them to make this outreach in a very deliberate way, in conjunction with TSA and with the contractor. Essentially, they're waiting for the green light on the go-ahead that, you know, once we have the schedule established, there will be a very deliberate process of informing people. It will start with a notice in the *Federal Register,* but there will be—you know, to make it official—but there will be all sorts of informal means, including these committees, to get the word out to people.

Senator CARPER. I think there's a disconnect here. Because the people who run our port, the folks who work there, believe there has not been good—in fact, the word was given to me as "poor" communication. So there are some differences between "excellent" and "poor." And, we always say, "The customer's always right." I'm not sure who the customer is here, but it could be the port and the folks that the port serves.

But, the message I would ask you to take back to your folks is, people in my port are not pleased with the communication with the program managers and I would just ask you to, let's do better. I know, everything I do, I could do better, and I suspect the same is true here. So I'd ask that you re-double your efforts. OK. All right.

Mr. HAWLEY. Yes, sir.

Senator CARPER. Could I ask just one more quick one? Thanks.

On one hand, we want to make sure that the folks that, whose background is such that would raise alarms and concerns—we want to make sure that they have a system here to catch those, to detect those folks.

At the same time, I'll be honest with you, folks who work at a lot of these ports, whether it's my port, or ports in New Jersey or other states, a lot of them you would look through the high school yearbooks, they weren't picked to be "Most Likely to Succeed," and a lot of them have had troubled pasts, they've—some of them have been in trouble with the law, some have been incarcerated, some have been pardoned, some have not. And, let me just ask, for the folks, for some people in the State of New Jersey this is the first good job they've ever had, and they've straightened themselves out, and they're staying out of trouble. How do we balance the desire, the earnest desire, to make sure that we're not allowing people who shouldn't be, who have a past that suggests that they shouldn't be allowed to have access to the port, and do pose a security risk, from those who just made bad choices in their lives earlier, and have straightened themselves out?

Mr. HAWLEY. It's a very, very, very important issue, because this is a credential to work. And, the standard is terrorist risk. And that is for what we all hope is an infinitesimal part of the population.

Our Hazardous Materials Endorsements in the trucking population is an analogy that gives me some confidence, because we've done 2.7 million of those, and the adjudication process, appeal, waiver process has been very effective, and has not been the problem we all might have anticipated. So, we are very, very zeroed in on that specific issue.

Senator CARPER. We want to work with you closely on that. Thank you.

Thanks, Mr. Chairman.

Senator LAUTENBERG. Thanks very much, Senator Carper.

One thing, and that is, according to the schedule as we've heard it, we're supposed to start issuing cards Monday in the New York/New Jersey region. And, it's now moved back, as I understood you to say, to somewhere in the fall. And, I don't think there can be a lot of optimism that this program is going to be meeting any of the targets outlined. We, you said, that the employee population

that may be covered could be 750,000, could be 1.2 million, or 1.5 million. Now, how do you plan to provide the resources, depending on what number you finally come up with?

Mr. HAWLEY. Yes. The program is scaleable. Using Port of Wilmington as an example, we've already hired the 8 trusted entities who will do the enrollment. That is part of the communication with the port, to identify how many people are going to be enrolled when the team goes in, and then they scale up to do it. So, I think, of the concerns, that is not one of the major concerns. I think we'll be able to handle the population. The part that is most important and still out there is the part Mr. Rabkin mentioned, in terms of the extensive testing that is required for the system.

Senator LAUTENBERG. I really don't understand how these parameters are being dealt with, because to me they don't pass the early testing that we've done, and we're stuck in limbo, and we're going to ask the employees to pay $137 to get this card, but it may not be system-wide. You said that that person could take that card anywhere in the country and use it to gain access. But, also, I think the Admiral said that this isn't necessarily the terror watch list, but it could be for any other reasons as well. Now, if this is going to be presenting a person's full background, looking at this card, this has got several tests it has got to pass so that one's liberties aren't encroached upon.

I'm sorry, but we have another panel here, and we are going to have a vote soon. So, I would ask that the second panel of witnesses be seated.

Thank you very much for being here with us.

Mr. Pomaikai, Mr. Michael Rodriguez, please take your seats. Thank you.

Ms. Himber is Vice President of the Maritime Exchange for the Delaware Ricer and Bay, the Maritime Exchange is the industry trade association for the Delaware River port system, including ports in Camden, New Jersey, and Philadelphia, and we thank you for joining us today, Ms. Himber.

Mr. Pomaikai is the Assistant Port Captain for Sause Bros., Incorporated, in Honolulu, Hawaii, and Mr. Michael Rodriguez, Executive Assistant to the President of the International Organization of Masters, Mates and Pilots. And we thank all of you for being here.

We're going to ask you to summarize your statements within a five-minute time range, if there's another minute needed, we'll permit that, but otherwise it will encroach on the other person's ability to have the microphone. So, Ms. Himber? Thank you.

STATEMENT OF LISA B. HIMBER, VICE PRESIDENT, MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY

Ms. HIMBER. Good morning, and thank you for inviting me to present testimony today, particularly on behalf of our members in New Jersey and Delaware, who have been involved in the TWIC pilot program since its inception in 2002.

Our members of the Maritime Exchange, include both private and public regulated facilities, as well as vessels, and the individuals who need access to secure maritime areas.

I've been involved with the TWIC Program for its—since the beginning—and in addition, as a member of the National Maritime Security Advisory Committee, have chaired two working groups developed to address TWIC issues.

And, I believe everybody's aware of the many setbacks, we've talked about some of them today. My feeling is, despite the setbacks which occurred in the past, the pilot program did allow TSA to gain an understanding of the challenges that they will face in implementing a program of this magnitude.

My testimony today will focus on issues surfacing from the TWIC rulemaking, as well as concerns relating to the second part of the program, the use of the TWIC readers at ports and vessels.

In drafting its final rule, it is evident that stakeholder comments to last year's proposed rule were given serious consideration. Particularly, we believe DHS made exactly the right decision to separate the card issuance, and reader installation processes. Yet, obviously in a program of this scope, there remain additional concerns about the program.

First, the rule is silent on casual labor, which is such an integral part of maritime operations that it must not be overlooked. While the rule does provide for accommodation for escorting non-TWIC holders, there's no clear pathway to implementing the escort requirement in any practical manner. In addition to the operational and physical impediments, other questions have arisen about the escort's liability and responsibility.

Similarly, our members are concerned about access for non-TWIC holding truck drivers, especially during the initial program roll-out.

The second major concern we have relates to the costs, which simply stated, and as you've stated, are too high. There's little incentive for individuals to seek employment at maritime facilities when the cost of such an employment may exceed his wages for the day. And, if the company pays—and some trade union agreements require that they do—it may cost several thousands more beyond the cost of the card to pay for meals, and time spent applying for and retrieving the card.

Significant additional costs will accrue for companies to escort non-TWIC holders. This is particularly troublesome given that some employers or employees may pay for cards that the individuals never receive, as a result of their security threat assessments.

Another question has been raised regarding processes for individuals who, for religious reasons, may not have their pictures taken, or must have their heads covered when being photographed.

These are just a few of the concerns which have surfaced over the last several months, and there are many others.

On the other hand, there are issues industry has voiced in the past as preventing successful TWIC implementation, and we would like to compliment DHS on the steps that they are taking to address them.

Predominant among these issues is—as everybody has mentioned today—has been the problem of communicating information to stakeholders, particularly as it relates to program setbacks and delays. But, we appreciate the creation of the TWIC Stakeholder Communications Committee, and look forward to seeing some improvement in that regard.

In addition, our local Coast Guard sector, Delaware Bay, has done an excellent job in facilitating outreach and sharing information as it becomes available.

Further, we've also been concerned that many TWIC technologies were excluded from the pilot program tests, and we are pleased that DHS will conduct an additional pilot. And for that, I'd like to talk for a minute about the card readers.

One of the key concerns submitted to the proposed rule related to the use of contact cards in the maritime environment. In response, the National Maritime Security Advisory Committee was asked to develop recommendations for a contactless TWIC reader, and we completed that work in February. There was one critical area where DHS and the maritime industry could not come to terms, and that's whether or not the fingerprint template should be encrypted. This may very well be one of the single-most important issues DHS will have to address as it enters the second phase of the TWIC rulemaking process.

Industry believes that individual privacy is more than sufficiently protected by virtue of the fact that the TWIC will not contain a full fingerprint image. There are other outstanding issues surrounding the selection and use of card reader technology, such as the use of a PIN, integration with existing port access control systems, and future expansion of the card, just to name a few.

In addition to addressing these and other remaining questions, we suggest that DHS revisit its approach to the TWIC reader implementation. The Department should first make the final TWIC policy decisions, such as the use of readers at low-risk facilities and vessels, or access control recordkeeping requirements, and then identify the technology that we need to support them.

We also suggest that DHS work with industry in the pilot program design phase, as well as its execution and evaluation and the subsequent rulemaking process.

In closing, let me say that although there are still a lot of serious concerns, DHS has made progress in bringing this program to fruition. We remain committed to the TWIC Program, and want to continue to work with TSA and Coast Guard, to ensure there are no unintended consequences, and that the program is going to be deployed in the most secure and efficient manner possible.

And, that concludes my remarks, and I'll be happy to answer any questions.

[The prepared statement of Ms. Himber follows:]

PREPARED STATEMENT OF LISA B. HIMBER, VICE PRESIDENT, MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY

Good morning, Mr. Chairman, Mr. Vice Chairman, and members of the Committee. 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 non-profit trade association representing the members of the commercial maritime industry in Southern New Jersey, Southeastern Pennsylvania, and Delaware, and our mission is to promote commerce at Delaware River ports. We accomplish this by engaging on issues and developing programs to support the safety, security, economic viability and environmental health of the tri-state port complex. Included among our 300 members are those companies and individuals who operate, or provide service to, the 2,800 vessels calling Delaware River ports each year. Our membership includes regulated vessels, port authorities and private maritime facilities as well as the many businesses and individ-

uals who need access to one or multiple facilities to do their jobs on a daily basis—such as tug and barge companies, steamship agents, labor organizations, surveyors, line handlers, and trucking companies, just to name a few.

Although the Maritime Exchange is focused on activity at Delaware River ports, we address issues of national significance with our sister maritime organizations under the umbrella of Maritime Information Services of North America, known as MISNA, as well as through NAMO, the National Association of Maritime Organizations.

In addition, I serve as Vice Chair of the National Maritime Security Advisory Committee (NMSAC), which as you are aware was established under the Maritime Transportation Security Act (MTSA) of 2002. NMSAC has been actively engaged with the Department of Homeland Security on the Transportation Worker Identification Credential (TWIC) program since its initial meeting in March of 2005, and I'll talk more about our recent accomplishments in a few minutes.

I appreciate this opportunity to discuss the TWIC program and issues associated with implementation of the final rule issued in January of this year. TWIC has long been one of the priority Federal projects for my organization and our members in the Delaware River maritime community.

Background

The Exchange role in the port—Like most associations, the Maritime Exchange is an advocate on issues of concern to its members, much like a Chamber of Commerce. However, what sets the Exchange apart from a traditional trade association is its operating role in the port. The Exchange operates on a 24/7 basis, and one of our primary responsibilities is to collect, store and disseminate information on all commercial cargo ships moving through the port. We also serve as a maritime information and communications hub for the region, conveying messages between ships and their shoreside service providers as well as distributing Federal safety, security, operational, and procedural bulletins to the maritime businesses community. Because of the importance of this function, which we have been providing since 1875, coordinating information through the Maritime Exchange communications center has been incorporated into the Area Maritime Security Plan for Coast Guard Sector Delaware Bay.

In addition to our traditional Ship Reporting function, 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 public and private sector transportation partners through a centralized maritime intelligence system.

Development of a regional standard ID—Because the Exchange had demonstrated its ability to bring together the various maritime stakeholders to develop, implement, and use a community information system, several 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 and developed a set of requirements for what would become known as the Electronic Driver Identification (EDID) System. By September 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 December 2001, the Exchange, in partnership with the Port of Wilmington, Delaware, had identified funding to develop a pilot program, and success-

fully programmed and tested what would become the Delaware River ID (DRID) system. We subsequently received a Port Security Grant to expand this program.

It was because of this effort that the Delaware River was selected as one of the TWIC pilot program locations. It was generally agreed that if such a system could work effectively at Delaware River ports, with three states and multiple private and public port facilities, it could 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.

Members of the Delaware River port community participated in all three phases of the TWIC pilot program, beginning with the Planning Phase which spanned the Fall of 2002 through the Spring of 2003, the Technology Evaluation from May to October of 2003, and the Prototype Phase, which started in November 2004 and officially ended in June 2005, although TSA continued to support Delaware River sites well into 2005.

I believe everyone is aware that there were a great number of setbacks which plagued the TWIC pilot program, which was originally scheduled for completion in December 2003. Despite some of the problems encountered by the Transportation Security Administration, some of which were discussed at a hearing before this Committee last May, it seems clear that the pilot program did afford TSA with the opportunity to gain an understanding of what would be required to implement a program of this magnitude.

Moving Forward

Program Deployment—Card Issuance—The Final Rule published in January is an extremely complex document which many maritime professionals are still working to comprehend. However, we cannot emphasize enough that we believe the Department of Homeland Security made the right decision in separating the card application and issuance processes from the reader installation and usage processes. Taken separately, each of these components of the TWIC program is extremely intricate and creates multiple possibilities to unduly hamper maritime operations if not implemented in a thoughtful and deliberate manner; we appreciate that DHS is allowing sufficient time to address the challenges of card issuance prior to attempting to introduce the component of accessing and communicating with a central TWIC database, which was never tested during the pilot program. There is no doubt that had both phases been implemented concurrently, the transition to full program deployment would have been fraught with multiple unanticipated problems.

In drafting its final rule, it is evident that DHS took into consideration the thousands of comments submitted by maritime stakeholders in response to the Proposed Rule published last May. Several of the issues cited have been addressed, such as the need to accommodate temporary and seasonal workers, and the elimination of the formal employer sponsor relationship. In addition, the Coast Guard drafted a very clearly-written and helpful Navigation and Vessel Inspection Circular (NVIC) guidance document; and we appreciated the opportunity to comment on the draft document prior to its finalization. This is not an opportunity the regulated public often enjoys.

Needless to say, however, in a program of this scope, there still remain some additional questions and concerns about the regulation.

First, the rule is silent on the issue of casual labor, which is such an integral part of efficient maritime operations that it must not be overlooked. While the regulation and the draft NVIC provide accommodation to escort non-TWIC holders, there is no clear pathway to implementing the escort requirement. Foremost among the challenges is the fact most facilities operators within the Delaware River and elsewhere have determined that the secure and restricted areas defined in their security plans will be contiguous, such that the entire facilities are restricted.

The effect of that decision directly relates to the numbers of non-TWIC holders who may be escorted by any one-TWIC holder. As outlined in the draft NVIC, escorting in a restricted area is limited to five non-TWIC holders for every one TWIC-holding escort. In addition, unless this guidance changes in the final version, the escort must be constant and side-by-side (*i.e.,* no monitoring via video or random patrol). The impact of this can be seen in the following scenarios: at the hiring hall, a longshoreman offers to drive three or four day laborers to the pier to report for work. Upon arrival, these individuals may be assigned to work different ships, and therefore the TWIC holder is no longer in a position to serve as an escort for the others. Or perhaps one of the workers is a female and the TWIC holder is male;

surely he cannot be expected to stay by her side during the entire workday. In any case, it is not conceivable that one worker could escort even one individual, let alone several others, on a constant basis while still fulfilling his own responsibilities. In addition to the practical difficulties, in some cases the physical layout of the marine facility prohibits the ability of the card holder to fulfill his/her obligations. For example, while it is obvious where the vessel berthed, the final resting place of the cargo is sometimes several hundred yards—or even miles—away from the vessel in a storage yard, warehouse or transit shed.

Further questions have arisen about the escort's liability and responsibility. If an individual under escort causes a Transportation Security Incident or otherwise violates existing laws, regulations or facility/vessel policies, what is the ramification to the escort? This question has yet to be resolved, and depending on the answer, it may be difficult, if not impossible, to identify willing escorts.

Similar issues arise as they relate to truck drivers. Many drivers arrive at Delaware River ports from other parts of the country. Of necessity, until the program is fully implemented, these drivers will not have their TWIC cards, and with the sheer volume of trucks moving through facility gates every day, it is not feasible that facilities, importers, or others could provide resources to escort these drivers. Even after initial TWIC rollout is completed, there will always be random arrivals by drivers who had never previously hauled cargo to or from maritime facilities.

The card application and issuance processes are not designed to accommodate long-haul truck drivers. For example, during initial rollout, if a driver arrives at the Port of Wilmington, he can, and should, apply for his TWIC card at that time. Yet the processes require that he return to the place of issuance to retrieve and activate his card after the security threat assessment has been completed. Needless to say, the driver may be long gone from the area with no immediate opportunity to return.

Suggestions for addressing the above issues include: allow TWIC applicants to designate that cards be returned to a different enrollment center than that where the individual originally applied, or include a mechanism to mail a card to an applicant's office or home—or other appropriate location—after which the individual could return to a convenient enrollment location to activate the card.

In addition, facilities should be given the option to create a "temporary" credential or visitor's pass in lieu of requiring escorts. If appropriate, when the individual's identification documentation is validated, his photograph could be taken and other information entered into the facility access control system. If necessary, this information could be submitted to DHS. Such a mechanism might be designed along the lines of the Florida "5 in 90" rule: Florida State regulation allows for a temporary credential, and if an individual presents himself for access to a regulated facility more than 5 times in 90 days, he or she would no longer be eligible for a visitor's card and would be required to obtain a Florida card. Needless to say, both DHS and the maritime industry would need to agree to mutually acceptable details to implement such a program within TWIC, but the idea bears consideration.

A second major concern relates to the cost of the TWIC card. Simply stated, the cost is too high. Although we anticipated there would be a significant cost saving associated with DHS centralizing the purchasing and production of the cards, these do not appear to have been realized. Again, keeping in mind that the maritime industry is highly reliant on casual, seasonal and temporary workers, there is little incentive for these individuals to seek employment at maritime facilities and vessels when the cost of such employment may exceed his wages for the day. Non-profit organizations, such as the Seamen's centers are also greatly impacted by the high price tag. At the Seamen's Center of Wilmington, where I serve on the Board of Trustees, the estimated cost to obtain TWICs for volunteers is $8,000; this represents an 8 percent increase in operating expenses for the upcoming year. Also, of particular concern is the fact that an applicant is required to pay the full price at application, even if he/she is subsequently denied a card and it is never produced. TSA should charge only the cost of processing the enrollment application and for the security threat assessment, with the balance to be paid only after the card is produced and activated.

Third, one additional question has recently surfaced in our region: how can we process TWIC applications for individuals who for religions reasons may not have their pictures taken or require that their heads be covered when photographed? While I would not hazard a suggestion on how to address such an issue, it may not have previously been considered and is certainly a challenge DHS will need to address.

These are just a few of the questions and concerns which have been raised over the last several months; there are countless others—far too many to address today. However, we expect that many of these will be resolved when the final NVIC is released.

In addition, there are a few issues the Maritime Exchange and others have raised in the past as preventing successful TWIC implementation, and we compliment DHS on the steps taken to address them.

Predominant among these has been the problem of successfully communicating information to the maritime industry—particularly as it relates to program setbacks and delays. We appreciate that that the Lockheed Martin contracting team has established a TWIC Stakeholder Communications Committee specifically to address the issues of communications. To date, the Committee has held only one meeting, so we are not yet in a position to evaluate its effectiveness; however we remain optimistic and look forward to working with the TWIC team toward a successful and smooth implementation.

In addition to efforts underway at the national level, our local Coast Guard personnel, who are responsible for coordinating activities between TSA, the contractors and the maritime community, have done an excellent job over the last several months in facilitating outreach sessions, helping identify enrollment center locations, and providing maritime stakeholders with information as it becomes available. We are confident that local Coast Guard will approach the implementation and, ultimately, enforcement of the TWIC program with the flexibility it demands.

In addition, during the last 5 years, many have held the belief that the constant turnover in DHS, TSA and TWIC program office leadership has contributed significantly to the ongoing delay in implementing the program. Over the last year, the personnel roster has been completely stable, and we are pleased to note that DHS seems to have addressed some of the internal issues associated with employee turnover.

Finally, the Exchange and others have expressed concerns about the fact that many of the critical technologies, such as communication with the database, use of biometrics, or individual (*versus* corporate) program enrollment were not tested, or tested insufficiently, during the original TWIC pilot program. We appreciate that DHS, as required by the SAFE Port Act, will conduct a TWIC pilot program to test reader technology and processes.

Installation and Usage of Card Readers—As stated previously, DHS elected to defer this component of TWIC implementation. We enthusiastically applaud this decision and appreciate the efforts of DHS to work with industry to determine the appropriate technology for use in the maritime environment.

One of the key concerns expressed by those commenting on the Proposed Rule last Spring related to the use of contact cards. Requiring that a card be swiped at a TWIC reader would not only significantly delay maritime operations, but contact readers are more susceptible to failure due to environmental elements, and they also present an easy and attractive target to vandals. In response, last November DHS asked the National Maritime Security Advisory Committee to develop recommendations for a contactless card reader which could be used at ports and vessels.

NMSAC agreed to accept this challenge, and it was my pleasure to co-chair the working group established to develop the recommendations. The Working Group included approximately 130 individuals, not including the Federal Government participants, and was organized into a maritime team and a security technology industry team. The maritime group was comprised of public and private terminal owners and operators, vessel owners and operators, maritime labor and employer organizations, trade associations, and a host of others. These individuals, with counsel of the security industry team members spent the months of December 2006 and January 2007 developing a series of operating requirements which would guide the development of the technical documentation. This document was completed by mid-February in advance of the February 28 deadline established by DHS.

For the most part, the technical team was able to meet the requirements outlined by the maritime industry representatives, and the technical specification endorsed by NMSAC reflects the combined efforts of the full working group.

However, there remains one critical area where the DHS and the maritime industry could not come to terms. This relates to the level of protection which should be placed on the fingerprint template transferred between the TWIC card and the reader. This is one of the single most important issues DHS will have to address as it enters the second phase of the TWIC rulemaking process.

In its simplest form, DHS has stated that the fingerprint template is to be encrypted; the maritime industry holds that individual privacy is more than sufficiently protected simply by virtue of the fact that the TWIC will not contain a full fingerprint image but only a minutiae template which cannot be re-generated if it is "stolen" during contactless transmission.

The following text is excerpted directly from the NMSAC recommendations:

A. *Privacy and Security Considerations*—NMSAC supports the inclusion of measures to protect individual privacy and acknowledges that this prerequisite, along with the need to enhance commerce and improve transportation security, has been included as a required goal of the TWIC program since it was announced in February 2002.

It is our understanding that all personally identifiable information about an individual gathered during enrollment will be retained by TSA in its central data bank. The card itself is expected to show and/or contain a photo, a unique cardholder identification number, and the individual's biometric fingerprint template.

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

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

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

In summary:

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

Therefore . . . "*Given the limited amount of information transmitted between the TWIC and the reader, the Working Group does not believe encryption will provide any additional security benefit, but it will increase both cost and processing time.*" The NMSAC TWIC Working Group (TWG) closely studied the issue and as a group concluded that the operational complexities increase by a level of magnitude and to the point where they are not proportionate with any perceived benefit of encrypting the biometric template. In short, there is no empirical evidence that encrypting the fingerprint template affords any additional protection of personal privacy.

DHS published the NMSAC recommendations for public comment, approximately 30 organizations or individuals responded, and an overwhelming majority agreed with the NMSAC on this critical issue.

While it is possible that a compromise solution to this challenge may be identified, the NMSAC group was unable to explore these opportunities given the fact that DHS did not provide any indication that it would expressly require encryption of the biometric until February, after the maritime team had completed its work. Further, DHS has not effectively presented rationale for taking this position; indeed, the original task statement presented by DHS stated that the recommendations shall incorporate "*reasonable* security and privacy controls," which we believe the NMSAC-endorsed recommendations did.

There are several other outstanding questions and concerns surrounding the selection and use of card reader technology. These include the use of a PIN during the TWIC verification procedures, integration with legacy access control systems, and future expansion of the card. However, we believe DHS will work effectively

with the pilot program participants and the National Maritime Security Advisory Committee to meet the challenges associated with this phase of the rulemaking process.

In addition to addressing the above, we suggest that DHS reverse its approach to the TWIC reader implementation. Specifically, rather than first developing a TWIC reader specification and subsequently finalizing policy decisions and promulgating a rulemaking on reader usage, we recommend that DHS first resolve the TWIC policy questions (*e.g.,* the requirement for use of readers at low-risk facilities and vessels, processes for enrolling individuals whose fingerprint cannot be captured, access recordkeeping, *etc.*), and then incorporate the appropriate technology to support them.

Finally, we suggest that DHS work with industry in the pilot program design phase as well as its evaluation and subsequent rulemaking activities.

Conclusion

Over the years, the maritime sector perhaps more than any other has recognized the need to implement new programs and practices in an effort to 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.

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

Senator LAUTENBERG. Thank you very much.

Mr. Paul Pomaikai, we welcome you.

STATEMENT OF CAPT. PAUL KAIPO POMAIKAI, SR., ASSISTANT PORT CAPTAIN, SAUSE BROS.; ON BEHALF OF THE AMERICAN WATERWAYS OPERATORS

Mr. POMAIKAI. Good morning, Mr. Chairman, and members of the Committee. Thank you for the opportunity to testify today, and for the support you have shown the industry.

My name is Paul K. Pomaikai, Senior, I am the Assistant Port Captain——

Senator CARPER. Excuse me, would you pronounce your name again, your last name, very slowly?

Mr. POMAIKAI. Pomaikai.

Senator CARPER. Pomaikai.

Mr. POMAIKAI. Pomaikai.

Senator CARPER. Thank you, sir.

Mr. POMAIKAI. Yes. I'm Assistant Port Captain for Sause Brothers, I also hold a Master's Ticket from the United States Coast Guard, going on my seventh issue.

We've come out of Honolulu, Hawaii. Sause Brothers has been in marine transportation business since 1937. Our Hawaiian Island division was incorporated in 1983.

I am testifying today on behalf of the American Waterways Operators, the national trade association for the tugboat, towboat and barge industry.

Mr. Chairman, Sause Brothers and other members of AWO consider ourselves partners with Congress, and the Department of Homeland Security in ensuring the security of our country. We take that responsibility very seriously.

We are here today because we have serious concerns about the impact of TWIC and the TWIC Program on our industry and the men and women who work in it.

These issues are very personal for me, I grew up in the maritime industry. My father was on the dock at Pearl Harbor on that fateful day, December 7, 1941.

My wife, Donna Laurie, is also a licensed mariner, sailing in the engine room department on the container vessel LURLINE, of Matson Navigation Company, as we speak. In 2003, Donna and I founded the Wai'anae Maritime Academy, located at Leeward Community College, a unit of the University of Hawaii.

Our intention was to provide young people with the education and training to begin a career in the maritime industry. So far, we have graduated 180 cadets in 9 classes.

I love this industry, and I know what a wonderful place it can be to make a career. I do not want to see my industry or the people who work in it harmed by well-intentioned, but misguided government regulations.

Mr. Chairman, AWO has two major concerns with the TWIC Program. First, we are concerned that the process for obtaining a TWIC will become a barrier to entry that will discourage new hires from beginning a career in the maritime industry. This will compound the existing shortage of personnel for our vessels.

Second, we believe requiring card readers on small vessels like towing vessels will add no practical security value and should not be a part of the proposed rule that TSA and the Coast Guard will issue later this year.

Let me elaborate on these concerns, briefly. First, AWO is very grateful that the SAFE Port Act passed by Congress last year included a provision requiring an interim work authority for new hires. However, under the process laid out in the TWIC final rule, an individual cannot begin working under the new hire provision, until he or she has traveled to a TWIC enrollment center, which could be many hours away, and for some of us in Hawaii, an island away, make an application for TWIC and pay the $137 fee.

This is an enormous hurdle for a young man or woman or an older worker, looking to make a career change. It is also a problem for employers who need to be able to put new hires to work as soon as they have passed the drug screen and physicals.

If new employees are scared away from seeking employment in the maritime industry because of the burdens involved in applying for a TWIC, companies could be forced to tie up boats for lack of crew members to operate them. Given the importance of maritime transportation to the economy of Hawaii, and other states, this would be a very major problem.

As an alternative, we would propose that the process begin with a computerized check against a terrorist watch list, not a trip to the TWIC enrollment center, with an employees consent, the employer could enter his or her name, birth date, Social Security number into the Coast Guard's Homeport website, to initiate a check against a terrorist watch list.

Provided this initial screening turned up no red flags, the individual could be put to work on an interim basis. Later, once the new hire has had the taste of life and work on a vessel and sees that it will work for him or her, the mariner could be required to complete the TWIC enrollment process.

Second, AWO believes that the card readers should not be required on vessels with small crews, like towing vessels. The SAFE Port Act gives the Department of Homeland Security the authority to limit the card reader requirement to vessels with more than a certain number of crew, to be determined by that agency.

On a typical U.S. flag-towing vessel with four to ten crew members, all of whom are familiar to management and fellow crew members, an electronic card reader adds no practical security value. We strongly recommend that card readers not be required on vessels with less than 10 crew members.

Thank you, Mr. Chairman, thank you for the opportunity to testify.

[The prepared statement of Captain Pomaikai follows:]

PREPARED STATEMENT OF CAPT. PAUL KAIPO POMAIKAI, SR., ASSISTANT PORT CAPTAIN, SAUSE BROS.; ON BEHALF OF THE AMERICAN WATERWAYS OPERATORS

Good morning, Mr. Chairman, I am Paul *Kaipo* Pomaikai, Sr., Assistant Port Captain for Sause Bros., Inc., in Honolulu, Hawaii. I want to thank you for holding this hearing and for the support you have shown for our industry.

Sause Bros., headquartered in Coos Bay, Oregon, is a privately held towing company, carrying forest products, building materials and petroleum to and from Alaska and Hawaii and up and down the U.S. West Coast. We employ over 500 people, including 300 mariners as crew on our boats. Sause Bros. owns and operates a fleet of 35 tugboats and 25 barges, and has been in the marine transportation business since 1937.

Sause Bros. has been engaged in common carrier service to the Hawaiian Islands since 1966. Our Hawaiian Island division was incorporated in Hawaii in 1983 to more effectively serve Island customers. The Hawaiian fleet provides inter-island and Military Sealift Command towing services, and distributes West Coast cargoes to Island customers. Our Island barge fleet carries products ranging from lumber, plywood, sand, and containers, to heavy equipment and petroleum products. Our ship assist fleet has gained a reputation among the Island shipping industry for safety, reliability, and professionalism.

As Assistant Port Captain for Sause Bros., I am responsible for all of our operations in the Hawaiian Islands. In addition, in 2003, my wife, Donna Laurie, who is also a licensed mariner, and I founded the Wai'anae Maritime Academy, located at Leeward Community College at Wai'anae, a unit of the University of Hawaii, to provide young people with the education necessary to begin a career in the maritime industry. We have graduated 180 cadets in nine classes, and this May we will be holding our tenth class. One of our commitments to our students is to help them find employment on board vessels following their graduation. We help them to meet the qualifications and get the documents they need, and we also help them develop the lifestyle that allows them to be productive workers in the maritime industry or other places they may decide to go with their lives.

I am appearing before the Committee today on behalf of The American Waterways Operators. AWO is the national trade association for the tugboat, towboat, and barge industry. The industry AWO represents is the largest segment of the U.S.-flag domestic fleet and a vital part of America's transportation system. The industry safely and efficiently moves over 800 million tons of cargo each year with a fleet that consists of nearly 4,000 tugboats and towboats, and over 27,000 barges. Our industry employs more than 30,000 mariners as crewmembers on our vessels. While a few companies in the towing industry are relatively large, according to the U.S. Army Corps of Engineers, over 90 percent of U.S. towing companies are actually smaller than Sause Bros.

Mr. Chairman, Sause Bros. and the other members of The American Waterways Operators have been, and will continue to be, partners with Congress and the Department of Homeland Security in ensuring the security of our country. Immediately after the September 11, 2001 attacks, the members of AWO worked in cooperation with the Coast Guard to develop security plans for our vessels, even before they were required by the Maritime Transportation Security Act of 2002. We take security seriously, and we are proud of the fact that our vessels and their crews are considered to be the "eyes and ears" for the Coast Guard on our Nation's waterways.

Nevertheless, we have serious concerns about the impact of the Transportation Worker Identification Credential (TWIC) program on our industry and the men and women who work in it. Our primary concern is that the process for obtaining a TWIC card will become a barrier to entry into the maritime industry for new hires, and this will exacerbate an existing shortage of personnel for our vessels. We are also concerned that requiring card readers on small vessels like towing vessels will add no practical security value and should not be part of the proposed rule that TSA and the Coast Guard will issue later this year. Allow me to elaborate on these concerns.

The May 2006 NPRM contemplated a TWIC enrollment process taking 30 to 60 days. In its comments on the NPRM, AWO said that such a time-frame would "seriously impede the ability of companies to bring new mariners into the industry in a timely manner." AWO and many of the 2,000 other organizations and individuals commenting on the NPRM suggested that the Department of Homeland Security include an interim work authority provision in the TWIC rule which would enable new hires in the industry to begin working immediately once they have passed an initial security screening.

We are enormously grateful that the Congress recognized these concerns, and as a result, a provision of the SAFE Port Act, Public Law 109–347, signed into law on October 13, 2006, required the inclusion of an interim work authority in the final rule. The statute provides: "The regulations shall include a background check process to enable newly hired workers to begin working unless the Secretary makes an initial determination that the worker poses a security risk. Such process shall include a check against the consolidated and integrated terrorist watch list maintained by the Federal Government." This language embodied the request we had made in our comments to the NPRM and made mandatory a process to allow new hires to begin working after an initial screening *unless* there is a determination that the worker poses a security risk (emphasis added).

The final rule issued on January 25, however, does not follow the intent of the statute to avoid creating barriers to new hires entering the industry. The proposal would deny a new hire the ability to begin work *until* the expensive and burdensome application process for a TWIC has been completed. Under the process called for in the final rule, new applicants must first travel to a TWIC enrollment center to make application for a TWIC in person, as well as pay the TWIC enrollment fee of $137, before undergoing an initial check against the terrorist watch list.

For many applicants in Hawaii and other parts of the country, this trip to the TWIC enrollment center will not be quick, easy or inexpensive. In Hawaii, for example, an applicant might have to fly from one island to another simply to apply for a TWIC. In other parts of the country where there is not a TWIC enrollment center nearby, applicants will also have to travel significant distances in order to make the application. This process creates a very high barrier to entry for new entrants to the industry who are not sure whether a career in the maritime industry is right for them.

Under the final rule, the "initial" security screening can only occur *after* the applicant has gone through the time and expense of completing his or her application. At that point, the employer may enter the individual's information into the Coast Guard's Homeport website to obtain the results of the check against the terrorist watch list. The rule indicates that a response can be expected within 24 to 72 hours after enrollment is completed. The problem is that for new hires and their employers, the TWIC enrollment process is only one step in a larger process of coming to work in the maritime industry. The first thing a company does when a new hire makes application is put him or her through a drug screen. If he or she passes that test, the next step is a physical exam, followed by a reference check. In the real world, neither the applicant nor an employer will want to invest in a trip to a TWIC enrollment center until those steps are taken. What that means is that it could easily take more than a week before an applicant is ready to travel to an enrollment center and make application for a TWIC, and then wait an additional 3 days for the results of the terrorist watch list check to be available.

Mr. Chairman, we are concerned that requiring new applicants to undergo such a burdensome process will deter individuals from entering the maritime industry. My company, and companies like mine, provide entry level opportunities for high school graduates looking to begin a career in the marine industry as deckhands on our vessels. These men and women come to our company with a need to begin earning a paycheck and providing for themselves and their families right away. Faced with the burdensome requirements surrounding the TWIC process, many will seek employment in another industry where the barriers to entry are not so high. Even without the TWIC rule, we are struggling with a chronic shortage of personnel to man our vessels. AWO estimates that the annual turnover of entry level personnel

in the towing industry is 50 percent. New hires may find that they get seasick or homesick and choose not to continue with a maritime career. Companies must also evaluate an individual's ability to perform on the job. Both the new hire and the company must come to the conclusion that a career as a working mariner is the right "fit" for the individual and the company before a long term commitment is made. For many new hires, the first manifestation of that commitment is the trip to the TWIC enrollment center and the payment of the application fee. That commitment should not be required until both the company and the applicant have concluded that the individual will continue in the industry.

In this environment, we are very concerned that the burdensome requirements for obtaining a TWIC card will exacerbate the current personnel shortage and could even force companies like ours to tie up boats for lack of crewmembers to operate them. Such an outcome would have a very negative impact on our ability to deliver the cargoes that are the building blocks of the economy in Hawaii, and would have the same negative impact on the national economy by affecting hundreds of towing companies around the country that also deliver the goods that are essential to maintain America's economic vitality.

As an alternative, we would propose that the process begin with a computerized check against the terrorist watch list, not a trip to the TWIC enrollment center. (This could be done concurrently with the drug screen or physical exam described earlier.) With an employee's consent, the employer could enter the new hire's name, birth date, and Social Security number into the Coast Guard's Homeport website to initiate a check against the terrorist watch list. Provided this initial screening turned up no red flags, the individual could be put to work on a vessel on an interim basis. Later—once the new hire has a taste of life and work on a vessel, and sees that it works for him or her—the mariner could be required to complete the TWIC enrollment process.

Another significant concern for the towing industry is the potential requirement for TWIC card "readers" on every towing vessel. The NPRM proposed a requirement for readers at both facilities and vessels. The Department subsequently announced that the card reader requirement would *not* be implemented as part of the initial TWIC rule but would be considered further as part of a separate rulemaking. This was a proper response to the many comments that were received about the card reader requirement, but the issue of card readers for towing vessels remains an open one.

Card readers are simply unnecessary for towing vessels. As AWO pointed out in its comments on the NPRM, crew sizes on tugboats and towboats typically range from four to ten mariners. In a typical U.S.-flagged towing vessel operation, every employee is known to management and fellow crewmembers. A stranger onboard the vessel is immediately obvious. Personal knowledge of fellow employees provides a higher security standard than reliance upon an electronic reader, no matter how sophisticated the technology employed. Access control procedures can be included as part of a vessel security plan. The validity of TWIC cards can be checked through means other than mandating computerized equipment onboard each vessel to constantly communicate with the database.

Mr. Chairman, even if card readers could be operated reliably in the severe marine environments where towing vessels routinely go—and that has not yet been demonstrated—there is simply no need to require their installation on every towing vessel in order to ensure the security of those vessels, or to ensure the security of the maritime transportation system. The SAFE Port Act gives DHS the authority to limit the card reader requirement to vessels with more than a certain number of crew, to be determined by the agency. On behalf of AWO, I would like to suggest that, at a minimum, vessels with 10 or fewer crew members requiring a TWIC should *not* be required to have a card reader installed onboard.

These problems with the TWIC program are very significant, especially for the many small businesses in the towing industry. They also have serious implications for companies throughout the towing industry and for the economy we serve. The provision for an interim work authority for new hires into the industry must be a workable one. The requirement to begin the process by traveling to a TWIC enrollment center must be eliminated. Failure to do so will have a significant negative impact on the ability of vessel operators to attract and retain the individuals necessary to crew their boats. In addition, card readers provide no additional security value in a small vessel environment and should not be required for vessels with ten or fewer crewmembers.

Mr. Chairman, I very much appreciate the opportunity to appear before you today. AWO and its member companies stand ready to work with this committee and with TSA and the Coast Guard to ensure the security of our country while

keeping mariners working, vessels moving, and the commerce of the United States flowing. Thank you.

Senator LAUTENBERG. Thank you very much for your testimony and the wonderful story about how you built a business and the important services you render. We congratulate you for that.

Mr. POMAIKAI. Thank you.

Senator LAUTENBERG. Mr. Rodriguez, please.

STATEMENT OF MICHAEL J. RODRIGUEZ, EXECUTIVE ASSISTANT TO THE PRESIDENT, INTERNATIONAL ORGANIZATION OF MASTERS, MATES AND PILOTS, AFL–CIO

Mr. RODRIGUEZ. Yes, Mr. Chairman, thank you.

I have submitted written testimony to the Committee. I'd like to read a brief statement to highlight a couple of points.

Senator LAUTENBERG. I would point out, Mr. Rodriguez, thanks for the reminder, that your full statements will be in the record as written, and that the summary—we hope—covered the points you wanted to make. But, be assured that your full statement will be in the record.

Please, Mr. Rodriguez, start.

Mr. RODRIGUEZ. Thank you, Mr. Chairman.

I am Michael Rodriguez, Executive Assistant to the President of the International Organization of Masters, Mates and Pilots. I began my career in the maritime industry in 1979 as a graduate of the United States Merchant Marine Academy at King's Point.

I sailed as a Deck Officer aboard U.S.-flag vessels until 1995. At MMP, I report on regulatory matters to the organization's leadership. I have been monitoring the development of the TWIC Program since the beginning.

I am also a Lieutenant Commander in the United States Naval Reserve, and a Veteran of Operation Enduring Freedom. I'll touch on a couple of points that are in my written statement.

The TWIC Program must be a national program. We believe Congress envisioned a national maritime security system that would pre-empt state and local systems. However, current provisions allow state or local governments to impose their own duplicate systems. This will result in higher costs and additional burdens for our workers and vessel operators as they trade between States, even between facilities, within the same state. We are also concerned about processing delays at the state and local levels.

The TWIC Program should be compatible with international systems. We have argued that the TWIC Program should take advantage of proven biometric technology by using the International Civil Aviation Organization standards. The ICAO standards are simple, efficient, and recognized worldwide.

Machine-readable travel document control systems used by the United States for electronic passports that monitor entry of foreign travelers into the United States employ the ICAO standard. We feel the ICAO standard is the logical choice for a biometric security card that could be interoperable with the TWIC and the Seafarer's Identity Documents that will be carried by crews of foreign ships trading to the U.S.

Finally, we are concerned about the administrative law judge program that would be put in place to handle denials and waivers.

We feel it is imperative that a sufficient number of ALJs be in place to handle the increased case load generated by the TWIC. If reviews are not processed in a timely manner, there will be a substantial negative impact on workers who are wrongly denied their TWICs.

That concludes my remarks, Mr. Chairman, I look forward to your questions.

[The prepared statement of Mr. Rodriguez follows:]

PREPARED STATEMENT OF MICHAEL J. RODRIGUEZ, EXECUTIVE ASSISTANT TO THE PRESIDENT, INTERNATIONAL ORGANIZATION OF MASTERS, MATES AND PILOTS, AFL–CIO

I want to thank the Committee for inviting the Masters, Mates & Pilots (MM&P) to present our views concerning the implementation of the Transportation Worker Identification Credential (TWIC) in the maritime sector. Our organization represents Ship's Masters and Licensed Deck Officers and Engineers working aboard U.S.-flag commercial vessels operating in the international and domestic trades, and on the inland waterways; and on civilian-crewed ships in the government fleet. The MM&P also represents harbor pilots.

The MM&P and, in fact, all the American seafaring and longshore unions, have a vital interest in maritime security and the administration of the maritime security regime. The members of our maritime labor organizations will be directly affected by any breach of maritime security. Many of the members of the MM&P also serve as Ship Security Officers and are responsible for the implementation of the U.S. Maritime Security Regulations and the International Code for the Security of Ships and of Port Facilities (ISPS Code).

Our comments are from the perspective of mariners who are continually in transit between different terminals, ports, states and countries for long periods as they work and live aboard their vessels. Accordingly, and in order to do their jobs efficiently and effectively, these maritime workers need consistency between national and international identity credentials, and uniformity with respect to the administration of access control.

Once fully implemented across all sectors of the transportation industry, the TWIC program will affect millions of American workers. In fact, many of our concerns are shared by other transportation workers, such as longshoremen, truck drivers, rail crews, ship service personnel and others whose employment is not limited to a single facility or port.

Seafaring and longshore workers want secure ports and vessels. We should be and we want to be treated as allies in the war against terror and not as the enemy. Our members would be among the first affected by a terrorist attack directed at or using our Nation's maritime transportation system. Therefore, we understand that access control procedures, including identification cards, can be important tools in the effort to prevent terrorist acts against our maritime transportation system. We support initiatives to identify and bar from working in security-sensitive transportation jobs individuals who clearly pose a security risk.

The stated goals of the TWIC program are to improve the security of our transportation systems, ensure the flow of commerce, and preserve the rights of workers; workers who are essential participants in the supply chain and in its security. We believe very strongly that in order to achieve these objectives, the process of applying for and receiving a TWIC must be efficient and must not result in unnecessary burdens upon workers. TWIC cards will be used in a marine environment covering a vast and diverse maritime workplace and the program must not only account for and reflect this reality, but must be adaptable to a wide variety of circumstances. Unfortunately, we are concerned that in too many areas this is not currently the case.

An Overview of the Current Situation

Support for a National Program

We have no doubt of the need for a "biometric transportation security card" as mandated by Congress in section 70105 of the Maritime Transportation Security Act of 2002 (MTSA of 2002). Early on we saw the benefits of a single, national security system based on a comprehensive security record check that could be used in a uniform system by a mobile workforce employed across many terminals, ports and states. Therefore, we support a system based upon background checks to ensure

that transportation workers do not pose a "terrorism security risk" to the United States. However, our support was predicated on the belief that such a system would be a national system that would become the standard for all maritime workers throughout the country and would prevent a proliferation of local systems that would all require their own background checks and fees. This unfortunately is not the case today. In the absence of Federal preemption, the program is permitting local requirements to overlay the TWIC standards for access control.

It should be clear that this situation is inconsistent with the goals of the TWIC program and unnecessarily burdens transportation workers who, by the nature of their work, require access to secure areas throughout a port, a state, the Nation, or even internationally. Terrorism and the prevention of terrorism are national, not local, concerns and the standards and system put in place to address these national concerns should take precedence over all others and not be left to the vagaries of each individual facility, port, city or state.

Need for International Uniformity

We anticipated and have urged that the TWIC program should take advantage of proven biometric technology by using standards developed by the International Civil Aviation Organization (ICAO). ICAO is the United Nations organization that regulates international air transport. The ICAO standards are simple, efficient, widely used and recognized worldwide.

In addition, the ICAO standards form the basis for secure identity documents recently adopted by the International Labor Organization in Convention 185 (ILO C185), Seafarer Identity Documents (SID). They also form the basis for the machine readable travel document control systems used by the U.S. for electronic passports that monitor access of foreign travelers to the U.S. It seems to us the ICAO standards are the logical choice for a biometric security card that could be used in an interoperable system that could include both our national cards and the international cards that will be carried by the crews of foreign ships; a population of seafaring workers employed aboard the foreign flag ships that carry 95 percent of America's export and import trade in and out of America's ports. Also, foreign port workers on U.S. flag ships while working cargo or undergoing repairs in foreign ports are expected to carry ICAO-compatible identity cards.

Because our TWIC system will not be interoperable with international standards the vast majority of ships and crews in U.S. deepwater ports will not be covered under TWIC-based access control systems. In other words, U.S. ships working cargo in a U.S. port with U.S. labor will have to comply with United States Coast Guard (Coast Guard) security provisions while a competing foreign ship with a foreign crew at the same terminal will be exempt—a situation we can begin to rectify by requiring that the TWIC system use the readily available ICAO standards.

An Overly Complex Card

It is disappointing to us that the very clear provisions regarding security cards in the MTSA of 2002 have still not been fully implemented in 2007. We attribute this to a number of factors.

First, ownership of the program has been split. Responsibility for the design of the card lies with the Transportation Security Administration (TSA) while the Coast Guard is responsible for implementation of access control programs using the TWIC.

Second, rather than accepting the proven ICAO standard, the TSA has adopted a design standard that is technologically sophisticated but overly complex and with a functionality that is, in most cases, far beyond that needed to comply with the MTSA of 2002.

Third, the card design standard and required supporting equipment is unproven in the maritime environment. Many individuals and organizations experienced in maritime transportation believe that the complex access control regime it is intended to support is both unnecessary and impractical throughout much of the maritime workplace.

Many have also raised objections over the approach taken by the TSA but, from our perspective, the agenda seems to be dictated by the concerns of the card manufacturers and contractors rather than by those of the affected population in the maritime industry who will be covered by the program. The result is a very complex and expensive program that we are concerned will cause major disruptions in the maritime transportation system if implemented as proposed. The cost for all this will have been borne by the workers in the system.

Leads to Overly Complex Control System

In May 2006, the Coast Guard issued a proposal for a security regime governing access control using the full functionality of the proposed card. That proposal met strenuous objections from the maritime industry which highlighted the proposed

card's impracticality. It appeared that the initial proposal was driven by a desire on the part of the Coast Guard to utilize the full alleged functionality of the TSA-designed card across the entire maritime sector regardless of any risk-based assessment of the threat of terrorism in the various sectors of a very diverse industry. As an example, vessels would be required to have onboard card readers interconnected via satellite communications to a central server maintained by the TSA to monitor use of the TWIC card. The impracticality of applying such a system to thousands of small inland towing vessels or offshore supply vessels, or even large ocean-going ships, should be self evident. While the initial Coast Guard proposed access control provisions have been withdrawn, they remain the subject of a future rulemaking that, as far as we know, still has the objective of utilizing the full functionality of the TWIC card across the entire maritime sector in a one-size-fits-all approach to security.

Security systems need to differentiate between high risk operations and low to no risk operations. Security regimes and controls must be scalable to the risk. For instance, a high profile cruise ship and a terminal handling thousands of passengers is in a very different risk category or tier than an inland towing vessel with a 5 person crew or a ship and terminal handling crushed rock or iron ore.

Need for Federal Preemption

Since transportation workers will be required to carry a TWIC, it follows that many of the card holders will travel between states, ports, and facilities. If the TWIC regulations allow each state, port, or facility to develop its own unique access control system that does not conform to a uniform national standard then the TWIC program will impose tremendous costs upon the industry and its workforce but provide no real value in terms of ensuring the free flow of commerce. The imposition of numerous inconsistent local requirements will require transportation workers to file numerous applications, undergo numerous background checks and pay the fees associated with all of the perhaps dozens of identity cards workers would have to carry. We are also concerned about delays in the various systems that would possibly deprive workers of employment while they wait for their cards.

Such a system clearly places an unreasonable burden on workers and on interstate and foreign commerce. We strongly believe there is an urgent need for Federal laws and regulations governing the TWIC to preempt any state or local requirements for such workers.

The TWIC Should Focus on Exposing Terrorism Security Risks

In the MTSA of 2002, Congress mandated that those who could be a "terrorism security risk" to the United Stated should be denied a security card. We agree with that standard and recognize that TSA has made some modifications to its original list of disqualifying crimes. We remain concerned that some of the broad descriptions of disqualifying offenses go beyond this standard. As this program is implemented over the next few months and years, we hope that TSA will indeed focus on preventing those that are genuine security risks from holding a TWIC and exercise appropriate discretion to not deny employment opportunities to those workers who may have simply made a mistake years ago.

Need for an Adequate ALJ Program

We are pleased that Congress has established a requirement for a review process before an administrative law judge (ALJ) for individuals denied a TWIC. It is our understanding that the present intent is to use the ALJ's within the Coast Guard system. We recognize the merits of having Coast Guard ALJ's conduct the reviews, but we have concerns as to the adequacy of the number of ALJ's within the present Coast Guard system to handle the caseload that may be generated. If the Coast Guard is not able to process reviews in a timely manner it will have a substantial impact on the ability of workers who may have been wrongly denied a TWIC, to earn a living and support their families.

Currently, the Coast Guard's ALJ system handles a caseload generated by approximately 200,000 credentialed mariners. It has been estimated that the initial surge into the TWIC program will cover approximately 850,000 workers. It is imperative that a sufficient number of ALJ's are in place to handle a vastly increased caseload.

Cost of the TWIC Program

We continue to oppose the concept that workers must pay the costs for the TWIC program. The security threat assessments and the background checks mandated by the final rule are considered necessary to enhance the security of our Nation's ports and are part of the overall effort to fight terrorist elements.

Security threats against ports and ships are actually aimed at governments and the public they represent, not the individual worker. Reducing security threats aimed at destabilizing our political and social institutions by terrorizing the public is primarily a role of the government. The general public is the principle beneficiary of maintaining a secure maritime transportation system and a secure global supply chain. Therefore, while we understand and appreciate the fact that some employers are paying these costs, the Federal Government should fund this program.

Privacy Concerns

As transportation labor has 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) of the MTSA of 2002 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." We do appreciate TSA and the Coast Guard's stated intent to fully abide by these privacy protections, but continued vigilance will be needed to ensure that sensitive information collected in the field, especially at so-called mobile enrollment centers, is adequately protected.

We also have concerns over discussions at the agency level toward allowing facilities to use the TWIC card for local applications. The idea is to store additional information beyond what is required by the MTSA of 2002. Such local applications might include employment records, training records, medical records, or other information of a sensitive nature and would defeat the national character of the system.

As a matter of privacy protection we strongly believe that the information on the TWIC should be limited to only that necessary for the Federal Government to comply with the security functions specified in the MTSA of 2002.

Conclusion

We thank you, again, Mr. Chairman for the opportunity to present our comments on the implementation of the Transportation Worker Identification Credential. We stand ready to work with you and your Committee and other concerned and affected parties to achieve a safer and more secure maritime transportation network.

Senator LAUTENBERG. Thank you very much.

And thank each of you for your excellent testimony. It helped focus in on the magnitude of this problem, and the consequences of what, if it is finally in place, what it might mean. So, it's important advice that you give us.

Mr. Rodriguez, how many states are moving forward with their own security credentialing programs in the absence of a Federal system? Have states begun aggressively to try to establish these identity systems?

Mr. RODRIGUEZ. Mr. Chairman, I'm aware of only Florida. That's my own knowledge. I could try to find that information for you and provide it for the Committee at a later date.

Senator LAUTENBERG. What do you think about the time frames discussed by the earlier, in the earlier panel for getting this program underway, any of you who feel that you have knowledge about that, please feel free to speak up, Mr. Rodriguez?

Mr. RODRIGUEZ. I feel that some of what Mr. Hawley's testimony touched on, the functionality of the card, the "Cadillac" sort of features it has, is holding us back in terms of getting a good system that we can test in operation.

What I mean by that is, we're talking about putting a lot of functionality into this card, and that's opening up the discussion to what we can put on the card? What sorts of information? Who gets to write to the card? That's slowing down the implementation. So, that's one of the reasons we would like to see the international standard adopted. It's a very simple standard, and once we get a program running, our recommendation is to build upon that, the capabilities that we need.

Senator LAUTENBERG. Either one of you want to comment on your view of the timeframe that has been discussed to getting this program really underway?

Ms. HIMBER. I—perhaps naively so, but am remaining cautiously optimistic—we do think that there is some momentum going, and we appreciate what the Secretary said about making sure we take the time now to make sure it works right, rather than rushing into it and dealing with problems later.

The experience that we've had with the pilot program is that that is the wrong approach. So, we're hopeful that once they do get started it will—the timetable that they ultimately develop, they'll be able to maintain, because they've worked out problems in advance.

Senator LAUTENBERG. So, your time frame is hopeful.

OK, Mr. Pomaikai?

Mr. POMAIKAI. Thank you, good morning, Mr. Chairman, again.

We have no problem with the time frame. The time frame is not a problem. What I fear is, the system will be inundated with a massive amount of people all at one time. If we roll the program out in certain areas like we are doing now, the Coast Guard has to deal with all of the merchant mariners going through their documents, going through background checks, probably drawing from the same database once the TWIC is implemented, they will again be swamped—and they'll have to deal with that problem.

Our problem is to be able to get new hires on the vessel in a timely fashion. They have to provide for their families, they have to go to work. They do so after a process of application with our company, and the process of obtaining from an MMD from the Coast Guard, there's a section there—section four of the application of the MMD—that calls for a background check. That process alone is done after the application is turned in to the Coast Guard, sent to Washington, reviewed by the Department of Homeland Security and the FBI. It comes back, allowing the mariner to, again, come to the Coast Guard REC and receive his MMD.

Now, the mariners go through an extensive process for that, and that is done on their own.

But, after all that he has done, he will have to go through the TWIC application process, not to mention——

Senator LAUTENBERG. Well, I think it's fair to say that the complications are not yet fully dealt with, and frankly, maybe not even thought about. So, this process has to protect to the—whatever extent possible, the people around the country the harbor supports from attack that could take lives, and really disturb the economies. On the other hand, we do have to get to work, we have hundreds of thousands, and the number, as you heard, varied between 750,000 and 1.5 million—it's a pretty good spread. But people that we have to work with, and a lot of these people are really itinerant in their work routines. People come in for a day or two or whatever as ordinary labor. But, we have to continue to pursue it.

The thing that I object to is the "pie in the sky" kind of deadline, or timeline that's expected. As I see it, based on the experience we've had so far, it's totally unrealistic. So, and we don't want it to be competing with other security measures that are, that have to be taken.

Ms. Himber, how many transportation workers do you think will require TWIC cards at the Delaware River ports?

Ms. HIMBER. I'm sorry to say, Senator, that I don't know that anybody has a really good feel for what that number is. We've talked about, you know, 75,000 direct jobs. That's just in the local region, it doesn't count truck drivers who come in from other regions that are not maritime areas, that might need to get their TWICs in our region. So, I don't know that anybody has the answer to that.

Senator LAUTENBERG. What's the expected beginning roll-out? When do they expect to be issuing cards?

Ms. HIMBER. I have heard the same thing that we talked about earlier in the Port of Wilmington which will be first, it's at least May, and perhaps later.

Senator LAUTENBERG. The complications are clear. We—thank you.

Senator Carper?

Senator CARPER. Thanks, Mr. Chairman.

I just want to say to Ms. Himber, Beth Osborne, remember, my staff who helps on these issues, is very complimentary of the work that you have done and expressed great pleasure in that, the relationship, and the way you approach your responsibilities.

Ms. HIMBER. Thank you.

Senator CARPER. You're the Vice President of the Maritime Exchange, is that correct?

Ms. HIMBER. That's correct.

Senator CARPER. Who is the President?

Ms. HIMBER. Dennis Rochford.

Senator CARPER. It must be a terrible burden to have to carry him on your back. How long have you worked there?

Ms. HIMBER. It'll be 19 years this year.

Senator CARPER. Probably seems a lot longer, I'm sure.

Ms. HIMBER. I was 12 when I started.

[Laughter.]

Senator CARPER. Small world, Delaware. Dennis and his family, we go to the same church together, so give him our best.

Ms. HIMBER. I will.

Senator CARPER. I want to follow up, first of all, if I could with you, let me just say, Mr. Pomaikai and Mr. Rodriguez, Commander Rodriguez—I'm an old Navy guy, too. My favorite rank was Commander. I loved being Commander Carper, I hope you get to be one, too.

Mr. RODRIGUEZ. I hope I get to be one soon.

Senator CARPER. You're close, how many years have you put in?

Mr. RODRIGUEZ. I've got 8 good in now, sir.

Senator CARPER. That's good. I take our Boy Scout Troop—my sons are Boy Scouts—we go to different service academies, and Senator Lautenberg, Senator DeMint and I get to nominate young men and women to go to these service academies, and we went to your academy last year. Had quite a good time.

What is your first name?

Mr. RODRIGUEZ. Michael.

Senator CARPER. I remember seeing scratched on one of the walls somewhere, and I think it was a girl's dorm, "For a good time, look up Michael Rodriguez."

[Laughter.]

Senator CARPER. I was wondering about that, so——

Mr. RODRIGUEZ. I can tell you, Senator, there are a couple of loose boards at the far end of the football field that say, "The Rodriguez Exit."

[Laughter.]

Mr. RODRIGUEZ. I don't think that's on the tour, though.

Senator CARPER. All right.

Ms. Himber, I think you were talking about the rule, you said the rule is silent on casual labor, do you remember?

Ms. HIMBER. That's correct.

Senator CARPER. Talk about that a little bit more for us, if you will, because there's a lot of casual labor at these ports.

Ms. HIMBER. The ports are completely reliant on casual labor, and particularly during, what we call, busy seasons, in the Delaware River, as you mentioned earlier, Chilean fruit season. You need additional, you need additional men to work the ships to handle the increased cargo flows that come in at certain times of the year.

You might have, in a season, at just one facility, 75 to 100 potential, what we call, casual workers, people who may come one day to work on a port, but you may never see them again. And that's throughout the maritime industry, not just in the Delaware River.

Senator CARPER. What do we do about those folks?

Ms. HIMBER. That's a big question that nobody, I don't think, has gotten the answer to that.

Senator CARPER. Well, maybe I should ask, what should we do?

Ms. HIMBER. Well, there are some options that are under consideration. The regulation, and the draft Coast Guard guidance documents allow that these people could be escorted. So, that any TWIC holder—perhaps another longshoreman, could escort one, to possibly ten, depending on the final decision, non-TWIC holders at any given time. We don't think that's practical, because the person who holds the TWIC, it's going to be difficult enough for him to do his own job while watching other people.

Other suggestions have included the idea of, perhaps, allowing for some sort of temporary credential that the port could issue, very similar to what ports are doing today with issuing a visitor's pass. How we could implement a program like that and still be in compliance with the legislation, we'd have to work through that, but that's an idea that we think would be worth looking into.

Senator CARPER. Thank you.

Mr. Rodriguez, two questions of you, if I could. I think you expressed some concerns about workers having to bear the cost of the issuance of cards, I think we're heard numbers as high as $150, or somewhere in that range. Do you think it's appropriate for workers to pay some portion of the cost of the issuance of these cards?

Mr. RODRIGUEZ. Well, from our standpoint, Senator, no. This is a function of government to provide this, and we believe that the Department should fund the program.

As Ms. Himber pointed out earlier, there are some workers, for whom, $137 is a day's pay. That's quite a bit of money.

Senator CARPER. Last question for you, if I could, Mr. Rodriguez. I think you mentioned how important it was that there is going to be an adjudication, there's going to be an appeals process. Folks are going to be denied a card, and they want to appeal, because of, maybe, a criminal record or some other issue. And you mentioned it was important that we have an adequate number of—what was it; administrative law judges? Is that what we're talking about?

Mr. RODRIGUEZ. Yes, Senator.

Senator CARPER. Talk about that just a little bit.

Mr. RODRIGUEZ. If a person is denied a TWIC because of the agency's action, then they have redress with the administrative law judge program. Our understanding right now is that the Coast Guard has seven openings for ALJs and there are only five slots filled. So, as this program begins to ramp up, and we start to look at the numbers, I heard 1.5 million today, I've been in discussions that say 2 million. So, there are another 500,000 on the table, possibly.

Senator CARPER. How many administrative law judges would there be to handle all of those?

Mr. RODRIGUEZ. My understanding at this time is there are five.

Senator CARPER. And, capacity for adding two more?

Mr. RODRIGUEZ. I believe there are those billets. Somebody else might be able to answer that.

Senator CARPER. Those are going to be very busy people.

Mr. RODRIGUEZ. They would be very busy people, sir.

Senator CARPER. Thanks very much.

Senator LAUTENBERG. Senator DeMint, welcome.

STATEMENT OF HON. JIM DEMINT,
U.S. SENATOR FROM SOUTH CAROLINA

Senator DEMINT. Thank you, Senator Lautenberg, and I thank everyone on the panel. We are embarking on a very difficult task, and I appreciate you adding your advice today.

We've heard many considerations and I'm sure there are many more we haven't talked about. Certainly we have to consider the workers and fairness to workers as we move forward with these TWIC cards. A lot of technical considerations, cost considerations, timing—a lot of things that you've brought up create huge challenges.

I just want to remind everyone, in addition to myself, that the whole purpose of all of this is security. That, as we look at our vulnerabilities as a Nation, we see our ports as one of those points of where we're most vulnerable. Where there's an opportunity when we look at weapons of mass destruction, of possibly moving through one of our ports, endangering millions of American lives, and all of this, in all of its complexity and difficult aspects comes back that we're trying to address a very real and new threat to our country. So, security is the purpose, and we've got to overcome these other problems.

I'd like to just address a question to Mr. Rodriguez, and again, I appreciate your testimony. As you know, no matter how much we spend, no matter how much technology we have at the port, such

as the scanning devices and sensing devices, no matter how many people we have, all it's going to take is one or two dock workers cooperating with terrorists, to circumvent the whole process. And, in order for a weapon to be smuggled into this country, a few people looking the other way can make that happen.

So, the people in our ports are terribly important. And that's what this TWIC card is all about; that we can do, at least a reasonable level of screening to know that we've done everything we can to keep a criminal element from working in our ports.

Because, we don't have to have someone who has committed a terrorist act before. Someone who has demonstrated his susceptibility to criminal activity could think that he's helping some pals smuggle in some drugs, when, in fact, it could be a weapon, a dirty bomb or something of that nature.

So, we've got a serious problem, the TWIC card is designed to try to screen out those people who might be susceptible to a criminal element. And my question is this, in the written testimony that you've provided, you've expressed concern about the broad descriptions of disqualifying offenses that you think go beyond the standard. What we've done in this requirement that excludes folks who've committed serious crimes, is adopt, pretty much, what we have at our airports at this point. What is in the language here now, in the regulation is very much like a bill that we've passed in the Senate, it did not survive conference. You say that we've got too broad a description. In fact, there is nothing broad about it. We have very specific listings of crimes that we think reach the threshold of criminal activity that we need to avoid in our ports, and I would just ask you if you could give me some of these disqualifying offenses that are listed, specifically in the regulation, that you think go beyond a reasonable standard.

Mr. RODRIGUEZ. Senator, one off the top of my head are crimes of dishonesty. I think that's quite vague, that's in the regulation.

Senator DEMINT. I don't believe that's in the regulation, is that in the regulation?

Oh, fraud, you're talking about——

Mr. RODRIGUEZ. Fraud.

Senator DEMINT. OK.

Mr. RODRIGUEZ. Fraud.

Senator DEMINT. Yes, sir.

Mr. RODRIGUEZ. The crime of robbery, we believe that in the MTSA the standard is the risk of terrorism, it might be arguable whether or not that really pre-disposes someone to be a risk for terror.

Senator DEMINT. I don't see that in the language, I don't know if you're using different words or not.

Mr. RODRIGUEZ. Well, then I need to address that.

Senator DEMINT. Oh, OK. I'm not trying to quibble. Again, these are very specific, as I look at the language of espionage and sedition, and crimes involving explosive devices and murder, and we have not picked small offenses, youthful indiscretions here in this language. We have tried to include things that indicate a serious bent towards criminal activity, and certainly I would be interested in any specific changes that you have, and if we've got something

such as misdemeanors in things that are listed, it's a change from what I've seen. Everything is specific in the language.

What I would just request from you, perhaps, is if you could send specific changes that you would like, back to the Committee, language that you think should be omitted and changed.

Mr. RODRIGUEZ. Senator, I'll be happy to do that. But I would like to make the point that we do feel that we have a starting point there, in the regulation. And that's where these disqualifying offenses belong.

Some of the testimony today, some of the reports we've been hearing are that we have this huge number of people that we don't really have a handle on yet. We want the flexibility in the hands of the TSA to make those changes. I'll certainly be happy to provide some language for you.

Senator DEMINT. Well, that would be helpful. Again, the point is not to punish workers who need a second chance, but our top security areas may not be the place to give some workers a second chance if they've demonstrated a susceptibility to criminal activity.

Because, as I've said before, if someone has been involved with drug smuggling, that is still a problem in our ports. If they think they're helping to smuggle drugs, but they're actually not smuggling drugs at all, we just need to look at that. And I think this is something that is apparently being contested, and we need to make sure that this is not something where we create an opening.

Again, all we have to do is make a few mistakes, and we've basically undermined everything we're working for. But thank you. Thank you, Mr. Chairman.

Senator LAUTENBERG. And I thank the witnesses for your statements. I found it particularly valuable. And, with that, this Committee hearing is adjourned.

[Whereupon, at 11:34 a.m., the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF KEN WELLS, PRESIDENT,
OFFSHORE MARINE SERVICE ASSOCIATION

The Offshore Marine Service Association (OMSA) thanks the Senate Commerce Committee for holding this hearing on the Transportation Worker Identification Credential (TWIC) program. We appreciate having the opportunity to submit the following testimony for the record.

OMSA is the national association representing the owners and operators of U.S.-flag vessels that support the offshore oil and gas industry. OMSA's members take their role in maintaining America's maritime security very seriously. They believe that the U.S.-flag vessel, owned by Americans and manned by Americans, is the heart of our domestic maritime security. It has often been repeated that the Coast Guard has designated the American mariner as its eyes and ears on the water. It created the Waterways Watch program to encourage those mariners to report suspicious activity. Efforts by the U.S. Government to encourage and facilitate the use of U.S.-flag vessels in U.S. waters make us all safer and more secure.

Conversely, actions that make it more difficult for U.S. flag vessels to operate or discourage U.S. citizens from becoming mariners have the effect of making us less secure. There is a growing fear in the maritime community that the TWIC program as it is emerging may disrupt vessel operations and become an obstacle to putting American citizens to work. If that were to happen, we would find that our security has been harmed, not enhanced.

The OMSA membership have a number of specific concerns about the TWIC program, but at this point, a primary concern for the maritime sector and for the Congress should be the lack of definition for the program even as it moves to implementation. The Final Rule on TWIC was published at the end of January after a short comment period and an inadequate opportunity for public hearings. In the less than 3 months since the rule was issued, it has required:

- Four published corrections;
- Three published addendum/clarifications;
- One additional rulemaking on card costs;
- One rulemaking on technical standards for touchless readers, a concept that was never included in the original Proposed Rule; and
- One draft Navigation and Vessel Inspection Circular (NVIC) on key elements of the implementation which should have been addressed through a formal rulemaking process, but were not.

There is still no public timetable for rolling out the program in the different ports and Coast Guard Sectors. Now the implementation appears to have been delayed by up to 6 months, but anxious mariners are still being told that they will need a TWIC card by September of 2008. A key component, the testing of TWIC readers, is still in its infancy and the substantial debate over those readers has yet to be held. All of this undercuts the integrity of the TWIC program and increases the skepticism of the maritime industry.

Looking at specific issues, a discussion of the impact of TWIC must begin with the recognition that the American mariners who crew U.S. flag vessels already undergo some of the most thorough background checks of any transportation workers in the world. This means that, with or without TWIC, U.S. seaman have already been checked out and approved by the U.S. Government to a standard that is at or above the level that TWIC will require. Ideally, the Department of Homeland Security should have been in a position to develop a program that built on what was already a successful process. Instead, the TWIC program and the mariner credentialing process were developed on two distinct tracks. While the Coast Guard is attempting to make those two processes operate concurrently, there is no avoiding the fact that they will require mariners to go through two separate processes, pay two fees and undergo two background checks.

It is important to note that any efficiencies in the background check process will have to wait for the development of a new Coast Guard Merchant Mariner Credential (MMC). There is no timetable for that MMC and, until it is released, mariners will still have to travel to a TWIC implementation center and undergo a background check for a TWIC card and then travel to a Coast Guard Regional Examination Center and undergo a subsequent background check for a Merchant Mariner Document (MMD).

The SAFE Port Act requires that the TWIC and Coast Guard mariner credentialing be conducted concurrently. As the processes of the TSA and Coast Guard are currently envisioned, this requirement of the law cannot be accomplished. This is because the agencies consider issuance of the TWIC to be a prerequisite for issuance of a Coast Guard credential.

If delays in implementation of the TWIC program continue, it may be worth revisiting whether the Merchant Mariner Document, with its rigorous background check, should be accepted as meeting the requirements of TWIC until that program has proven its effectiveness. This could be accomplished by simply exempting credentialed mariners from the requirement to obtain a TWIC for a period of time with the understanding that the Coast Guard will continue to do the background checks. Mariners could then be folded into the TWIC process once the large numbers of other maritime transportation workers have been processed and the Coast Guard MMC is in place.

Much has been said about the need for temporary work authority, a simple and expedient way to put mariners to work while their TWIC is being processed. The process that was made a part of the Final Rule does not meet the spirit or letter of the SAFE Port Act and is far too cumbersome and difficult to administer to meet the intent of Congress. The rule promulgated by the TSA addresses the requirement for temporary work authority by requiring companies to complete onerous paperwork if they want to grant employees unescorted access to MTSA regulated vessels or facilities. New hires after passing an initial security screen by TSA, and after companies complete the administrative requirements may then be granted "unescorted" access so long as they are "accompanied." The Rule does not adequately define either "unescorted" or "accompanied" in such a way as to give companies any confidence that their use of newly hired workers will be acceptable.

Other groups have suggested much simpler but effective approaches and we support those suggestions. However, we point out one nuance that should not be missed. Many mariners who would fall under this temporary worker concept will also need a Coast Guard credential. So far, the Coast Guard has been unwilling to also allow for temporary mariner credentials to go along with the temporary TWIC authorization. Mariners will need both and they will need the process to be simple and expedient. Unfortunately, any process that is not simple will result in more cost for the maritime industry and more hands-on activity by government agencies.

On a related note, a law change may be necessary to allow for the waiver for TWIC requirements in the event of a national emergency, such as a hurricane. Our industry's mariners experienced this problem firsthand with the loss of the Coast Guard's Regional Examination Center in New Orleans as the result of Hurricane Katrina. The Coast Guard has asked Congress to grant it the authority to waive license and credential expiration dates in these sorts of emergencies. It may also be necessary to waive TWIC expiration dates. Again, because the decision was made to require mariners to meet both requirements, any effort to mitigate the problems caused by a disruption of the government service will require that both TWIC and merchant mariner credentials be extended.

There are real concerns over the processing of TWIC applications. More information is needed on how the Transportation Security Agency intends to meet the staffing levels to expedite processing, especially as the estimated numbers of Americans required to obtain a TWIC card continues to grow. Clearly, many transportation workers will sail through the TWIC process without problems and will hopefully receive their TWIC card within the time-frames that TSA has estimated. Just as clearly, some potential workers will be permanently rejected based on the disqualifying offenses in the law. However, there will also be a third group that will fall somewhere in the middle. These individuals may have their initial application rejected because of errors or because they committed an offense that requires a judgment call by someone in government.

Focusing for a moment on individuals who may be rejected by mistake, we can only look at the TSA No-Fly List to see the problems that this could create. Much attention has been focused on individuals, including small children, Coast Guard officials and even U.S. Senators who have found themselves on the No-Fly List. Several years after the No-Fly List was created, TSA is still wrestling with how to best remove people who should not be on the list. TSA has been silent on how it will

ensure that maritime transportation workers will not be rejected in error or because they have the misfortune of sharing a common name.

Turning to workers who have committed an offense that requires some interpretation, the list of crimes that are not permanently disqualifying crimes is extremely vague. The primary example may be that of "dishonesty, fraud or misrepresentation." If a transportation worker was once convicted of using a false ID to purchase alcohol or for purchasing alcohol for a minor, those are regrettable offenses, but they do not make that individual a terrorism suspect.

As an example of this, Operation Drydock was the Coast Guard's comprehensive effort to ensure that mariners did not receive false documents. The exhaustive research into mariner credentials exposed several hundred instances in which mariners were not truthful on their applications. However, these were correctly judged to be efforts by those mariners to avoid admitting to a minor offense in their past. Action was only taken against a small handful of mariners who were judged to be truly fraudulent or potential security risks. The lesson was plain, there are and will be cases of dishonesty that should not be disqualifying events. Those workers should be allowed to obtain a TWIC, but it will take some form of human assessment to clear them. TSA should say how it will ensure that those applications are reviewed quickly and effectively.

Unfortunately, the TWIC appeal and/or waiver process could delay approval for these transportation workers for months. The procedures seem to be clearly designed to allow for denial due to a failure of the applicant to comply with the rules or time frames. There are no requirements for timely review or response by the TSA, or applicant review of detrimental information that is deemed "secret" by the government. At Congress' insistence, the rule allows for an appeal to an Administrative Law Judge, but given the limits on the ALJ resources, this will be a long process and may only be a "court of last appeals" for the most dedicated workers. It is likely that most entry level workers will have given up and gotten another job long before they have exhausted the appeals process.

Throughout the development of the TWIC card process, there have been numerous examples of the agencies ignoring well established vessel operations and imposing an unworkable approach. For instance, where the industry raised concerns over lost TWIC cards keeping mariners from going to work, the Final Rule says that a worker who loses a card will have 7 days in which to work while the replacement card is being processed. This ignores the fact that much of the maritime sector works a 28 day shift, making it impossible to apply for a replacement card and then go to work on the vessel.

The biggest unresolved aspect of TWIC involves the reader machines. The MTSA legislation that called for the creation of the TWIC program does not require the use of reader systems. The Final Rule makes it clear that the agency does not believe it needs Congressional approval to impose reader systems. The Department of Homeland Security has yet to make the case for how readers on vessels will enhance security, especially in a cost effective way.

In fact, the debate over readers has not yet happened. However, the planning for readers is moving ahead in advance of the debate and, we believe, in advance of the intent of Congress. The National Maritime Security Advisory Committee (NMSAC) assigned by TSA to develop a touchless biometric standard for readers cautioned TSA in its final report that prior to implementing any reader requirements that the public debate on the technology should be conducted. To emphasize this failing, a minority report was submitted to TSA *signed jointly by industry groups and organized labor* stating in part that ". . . TSA and Coast Guard should use the expertise of the various vessel operating communities to determine whether or not any use of TWIC readers is justified on any vessels."

The SAFE Port Act required that TSA perform a test of reader technology at facilities and on vessels and report back to Congress in 6 month increments until the pilot program is concluded. TSA has reported that it intends to use port security grants to fund the tests. This presents a number of practical problems. First, the port security grants are not generally open to vessel operators. Second, the agency has not made a concerted effort to engage vessel operators in these grants. Finally, by wedding the reader tests to the grant process, TSA has created a number of obstacles for vessel operators, such as:

- The reader machines do not yet exist, meaning that the vessel operator would have to find a manufacturer and oversee their construction.
- Lacking existing machines, it is difficult to determine how much money the grant applicant should request.
- There may be liability questions that cannot be anticipated but could emerge for a vessel operating company that becomes the grant applicant.

- There have been no common testing criteria, accepted procedures or control mechanism established.

The schedules for the testing and the schedule for the final rule are also in conflict. The Congressional timetable requires that the report of the tests be completed within 20 months, but TSA has said publicly that it plans to issue a final rule on readers in January of 2009 and that they will issue the reader rules independent of the study. Under these timetables, the users will be asked to comment and the agency will make a decision on a technology that it has not had a chance to adequately test and evaluate. Clearly this does not fit anyone's definition of sound public policy, especially for a testing program that has already been identified by the GAO as being problematic.

In discussing maritime operations we must stress that safety is the primary goal, trumping even security. Lives lost at sea by unsafe operations must be avoided. Requirements must be judged by whether they harm safety before they are blindly accepted in the name of security. Unfortunately, there has been little or no consideration of what the reader proposal might do to safety. For example, the NMSAC report on card readers indicates that they will be wired so that the "electrical signal from the panel used to command the door's electromechanical locking mechanism." Vessels do not have any such capability and years of experience have shown the danger of locking public access doors on vessels. It is the sort of fundamental acceptance of vessel safety that has been missing from the TWIC development.

OMSA's members operate vessels that have relatively small crews who have been specifically assigned by a company to serve on a specific vessel. Requiring one or, according to the proposed rule on TWIC, several readers on the vessel does not enhance security, but does dramatically drive up the cost of the program. Congress assigned the Commandant the authority to waive the requirement for smaller vessels based on crew size. OMSA's members believe this authority should be used in such a way as to exclude offshore vessels from the reader requirement.

Finally, one of TSA's implementation plans will significantly increase the cost of the program and has not received the attention it deserves. At a recent meeting of the National Maritime Security Advisory Committee, TSA officials indicated that they were finalizing the new standard for touchless reader systems and, when that standard was finalized, it would be necessary for every TWIC holder to return to a TWIC processing center to have his or her card reprogrammed. This unanticipated requirement will cost the offshore sector several million dollars alone in lost time and travel costs.

In conclusion, the maritime industry has a number of concerns about the TWIC program. The specific concerns need to be addressed, but there is a larger scale concern that the program is still ill-defined and does not have the support of the industry that will be most affected by it.

Thank you for allowing the maritime industry to submit testimony on this issue. We would be happy to respond to any follow-up questions the Committee may have.

PREPARED STATEMENT OF THE PASSENGER VESSEL ASSOCIATION

The Passenger Vessel Association (PVA)—the national trade association of U.S.-flagged passenger vessels of all types—appreciates this opportunity to submit testimony on the Transportation Worker Identification Credential (TWIC).

Our primary message is: TWIC will affect hundreds of employers and thousands of employees who are not engaged in international ocean cargo shipping. Therefore, the TWIC system must take into account the different circumstances of this segment of the maritime industry.

PVA understands and supports rational security measures. Many of its members' vessels operate in compliance with an approved security plan, as required by the Maritime Transportation Security Act. PVA has developed a Coast Guard-approved Alternative Security Program, as allowed by the MTSA rule. Yet, this implementation has been very expensive for our companies. Some have hired a Company Security Officer, a new position for them, to assist in the completion of risk-based threat assessments, identify vulnerabilities, and establish procedures to control access to the restricted areas of their vessels. PVA members have undertaken extensive training, drills, and audits. All of this work has costs associated with it. Still to come are the costs of TWICs, vessel-tracking Automatic Identification Systems (AIS), and perhaps TWIC readers.

Our members believe that a small company does not need an electronic TWIC card or a TWIC reader to know that employees Sam and Karly or Bill are who they say they are when they show up to work each day. They are the same Sam and Karly and Bill that the small company interviewed, hired and trained. They believe

that there are other methods that can be used to verify the status of identification that present little or no cost to the small employer.

Congress intended TWIC to focus on large ships that operate at commercial port facilities where the flow of cargo depends on numerous non-vessel, non-facility employees going in and out of the port. PVA does not believe that a small passenger operation such as operated by many of its members was ever envisioned by Congress to be included in the security concerns of America's ports.

Our Members Need To Put Individuals To Work Promptly

In our segment of the maritime industry, the ability to hire employees and have them go to work quickly is absolutely essential. Seasonal operators make up a large portion of our membership. Such an operator may hire seasonal workers for up to 80 percent of the staff, including deckhands, wait staff, and bartenders. The pool of potential employees includes students, teachers, and retirees. Clearly, these employees are not "professional" mariners. It is not uncommon for there to be 100 percent turnover of seasonal employees from 1 year to the next. These people may be hired only days before they begin work on the passenger vessel.

Our members compete aggressively with many other businesses for good seasonal employees. Our competitors for employees are hotels, marinas and restaurants, not subject to the TWIC requirement. Most of our seasonal employees are college or high school students who need a job when school ends to make the money they need for the next school year. This generally means they are available to the employer for approximately 90–100 days. They cannot apply for this summer employment and then wait 30 days for an ID card. They cannot even wait 2 weeks.

It is essential for the law and TWIC rule to recognize the "facts of life" regarding employees on domestic passenger vessels. The rule needs to accommodate the need to hire these folks quickly.

PVA acknowledges and appreciates the provision in the SAFE Port Act (section 104(c) of Public Law 109–347) mandating that the final rule allow employers to put newly-hired workers on the job pending the processing and issuance of a TWIC. That provision states: "The regulations shall include a background check process to enable newly hired workers to begin working unless the Secretary makes an initial determination that the worker poses a security risk. Such a process shall include a check against the consolidated and integrated terrorist watch list maintained by the Federal Government." The final rule attempts to comply by purporting to allow employers to put new hires to work with "accompanied" access to secure areas for up to 30 days once new hires have applied for their TWIC and an initial name-based check is completed. PVA remains concerned, however, as to how this provision will work in real life.

Reduce The Direct And Indirect Costs Of The TWIC

Most seasonal or temporary workers on domestic passenger vessel cannot afford or will not pay $137 for a TWIC, particularly when they have other job options that do not entail such a requirement. Congress must realize that domestic passenger vessel operators will be forced to pay the application fee for these potential employees, as they now pay for their pre-employment drug test, first-aid training, and security training, all currently required for their employees, but not required of the waterfront restaurant or the marina up the street.

There are other unaccounted-for costs of this rulemaking. One cost is the transportation costs for the employee to travel to the enrollment center. In fact, the employee must travel twice to the enrollment center, first to apply, then to pick up the TWIC. That means two round trips, costing gas, parking, and time away from the job. Not once, but twice! For many employees, the passenger vessel operator will have to provide this transportation when employees either don't drive or don't have transportation. Many would have to have Mom or Dad drive them. This is a roadblock to hiring good seasonal employees. If asked to make this trip, no matter who pays for it, most will simply chose to work elsewhere. It's just too much trouble for a summer job.

How many TWIC cards will be requested by applicants who change their mind and go to work at the restaurant down the street when they find out that the restaurant will put them to work right away? How many TWIC cards will be issued, and the applicant never picks up the card, because Mom decided the family was going on vacation instead? How many new hires will quit after the first day? These are the unintended costs for the small employer that we are concerned about.

WIC Enrollment Centers Must Be Located In Places That Are Not Traditional Ports

Also, PVA fears that the contractor will be inclined to locate TWIC enrollment centers only in large port cities. This will be where the contractor can achieve econo-

mies of scale to make a profit on the contract. However, in real life, many PVA operators are located in remote locations that are not considered to be major maritime centers—places like the islands of Kauai and Maui, Ketchikan and Kodiak in Alaska, Down East locations in Maine, Lake Tahoe and Lake Powell, and inland towns such as Omaha, Pierre, and La Crosse, Wisconsin. PVA has provided the Coast Guard and the contractor with a list of suggested places for enrollment centers that are not traditional maritime centers but that are necessary to accommodate our segment of the U.S.-flag industry. PVA urges the Senate to instruct the contractor and the Coast Guard that contractor profit can not be the only or even the controlling factor in the placement of TWIC enrollment centers.

No Burdensome Recordkeeping On The Employer

PVA also objected to the provision in the proposed rule to require each employer to keep detailed records for 2 years, showing every occasion on which an employee enters a secure area. This would do nothing to prevent security incidents, but would impose a huge paperwork burden on a small business. Why add a new redundant recordkeeping requirement, on top of the payroll records and vessel log books that our members already maintain? Fortunately, the Federal agencies deferred action on this proposal for now, but PVA urges the Senate to ensure that this bad idea is not resurrected.

Thank you for your interest in the special needs of the U.S.-flagged passenger vessel industry, particularly the hundreds of small employers in this segment who fall within the purview of the TWIC requirement. Congress, the Transportation Security Administration, and the Coast Guard must keep in mind that an appropriate level of maritime security can be achieved without unnecessarily harming American small businesses.

PREPARED STATEMENT OF THE MARITIME TRADES DEPARTMENT, AFL–CIO

The Maritime Trades Department, AFL–CIO, consists of 24 international unions and 19 port maritime councils in the United States and Canada representing approximately 5.5 million working men and women. The vast majority of those workers live and work in the United States. Virtually all of them stand to be affected by the Transportation Worker Identification Credential (TWIC) program, whether they work aboard vessels or in shipyards or elsewhere in the marine transportation sector.

The MTD thanks the Committee for this chance to convey our views on the implementation of the TWIC program in the maritime sector. The program is enormously relevant to our affiliated unions and their members. The MTD submits these comments on their behalf, with particular emphasis on the U.S. Merchant Marine:

Affiliates: Bakery, Confectionery, Tobacco Workers and Grain Millers International Union

International Brotherhood of Boilermakers, Iron Ship Builders, Blacksmiths, Forgers and Helpers

Communications Workers of America

International Brotherhood of Electrical Workers

International Union of Elevator Constructors

International Union of Operating Engineers

International Association of Fire Fighters

Glass, Molders, Pottery, Plastics and Allied Workers International Union

International Association of Bridge, Structural, Ornamental and Reinforcing Iron Workers

International Longshoremen's Association, AFL–CIO

International Association of Machinists and Aerospace Workers

Marine Engineers' Beneficial Association

United Mine Workers of America

International Union of Allied, Novelty and Production Workers, AFL–CIO

Office and Professional Employees International Union

International Union of Painters and Allied Trades of the United States and Canada

Operative Plasterers' and Cement Masons' International Association of the United States and Canada

United Association of Journeymen and Apprentices of the Plumbing and Pipe Fitting Industry of the United States and Canada

Seafarers International Union of North America

Sheet Metal Workers' International Association

American Federation of State, County and Municipal Employees

United Steel, Paper & Forestry, Rubber, Manufacturing, Energy, Allied Industrial & Service Workers International Union

Transportation • Communications International Union/IAM

The MTD acknowledges the scope, complexity, and challenge of protecting our Nation and our maritime transportation network from terrorists. We believe that a safe, secure and reliable maritime transportation system is vital to this Nation's economic, defense and national security. To that end, MTD affiliates have implemented many educational and training programs responding to the mandates of the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code and, further, have offered their assistance and views to the government in its efforts to devise and implement appropriate measures to protect this Nation and our transportation sector from terrorism.

The MTD generally endorses the concept contained in the statute for a biometric transportation security card. However, there are certain items within the implementation of the statute by the Transportation Security Administration that warrant our concern and comment. The MTD will focus its comments on those issues, as follows.

Merchant Mariner Document (MMD)

The MTD endorses the idea of a biometric transportation security card, as mandated by the Maritime Transportation Security Act of 2002. The MTD appreciates the efforts and time expended by the Transportation Security Administration in attempting to implement this requirement. However, we believe that the complicated and burdensome process finalized by the agency is both unnecessary for merchant mariners and may prove severely disruptive to maritime commerce.

As both the MTD and our affiliated unions have repeatedly advocated, the current Merchant Mariner Document could and should be modified to include an encoded biometric, to be used as a biometric transportation security card in lieu of the TWIC, especially since the Coast Guard recognizes the MMD as an identity document. We question the need for yet another document that the merchant mariner must obtain and carry when the current and time-tested Merchant Mariner Document may be adapted to encapsulate an encoded biometric. The MTD believes that with a security vetting process (threat assessment), preferably initiated by the Coast Guard, the biometric MMD would adequately respond to the mandate of the MTSA for a biometric transportation security card, given the fact that the Coast Guard advises that a security assessment is not required for the mariner population who have an MMD issued after February 3, 2003, implying that those mariners have undergone a full security vetting by the Coast Guard and therefore need not undergo a TWIC security assessment. The MTD urges the Committee to consider this simplified approach for merchant mariners who are required to hold Merchant Mariner Documents instead of agreeing to the TSA implementation process as enunciated in its final rule.

Further, the MTD believes that the Coast Guard itself has the authority to implement the biometric transportation security card mandate as recommended above. In fact, the MTSA requires the Secretary of Homeland Security to issue a biometric transportation security credential to merchant mariners. Section 102 of the MTSA defines "Secretary" to mean "the Secretary in which the Coast Guard is operating." It is our view that within this definition, the Coast Guard has the authority to issue an MMD with an encoded biometric as a merchant mariner biometric transportation security credential. Moreover, this would certainly negate the need for a change in the Code of Federal Regulations as proposed in *USCG–2006–24371, the Consolidation of Merchant Mariner Qualification Credentials,* currently being considered as a supplementary proposed rulemaking.

A further reason for utilizing a biometric merchant mariner document in lieu of a TWIC is the fact that the final rule proposes standards which will primarily impact merchant mariners and port workers. Why reinvent the wheel when a proven, time-tested, and internationally accepted document already exists that, with some modification, responds to the mandate of the MTSA? In addition, to date, there are no TWIC requirements for other workers in all modes of transportation. It is our view that if the TWIC is not applicable to all modes of transportation, then the sys-

tem is essentially flawed due to port intermodalism and the security objective is undermined.

User Fees

In its final rule, the TSA proposes to establish new user fees for the TWIC process. Although the MTD opposes a TWIC requirement for merchant mariners, we nonetheless state that it is patently unfair to impose yet another user fee on the merchant mariner for a credential that can be encompassed in the MMD. In fact, the merchant mariner is already charged a user fee for the process associated with the MMD. The MTD is aware that Section 520 of the 2004 DHS Appropriations Act requires TSA to charge a reasonable fee for providing credentialing and background investigations in the field of transportation. The principle behind user fees is based on the philosophy that beneficiaries of Federal expenditures should repay the government in the form of a user charge on all or a portion of the Federal expenditures incurred for a service. User fees are based on the premise that some agency services are of benefit only to particular segments of the population and that fairness dictates that these services be subject to user fees. However, the MTD contends that the TWIC program is not of benefit to a particular segment of the population—the merchant mariner in this case—but primarily in the interest of public security. It is our belief that one of the key criteria regarding the application of a user fee for TSA services rendered is whether the service provides a special benefit to an identifiable recipient *above and beyond* those that accrue to the public at large. In this case, it does not. Therefore, given the fact that obtaining a TWIC is in the interest of public security, merchant mariners should not be assessed a user fee. It. is neither fair nor reasonable to assess a user fee on a merchant mariner for a security mandate that has broader benefits. The background checks and security threat assessments contained in the implementing final rule are considered necessary to enhance the security of our Nation's ports and are part of an overall effort to fight terrorism elements.

Federal Preemption

The MTD recognizes and acknowledges the fact that states have the right to regulate access to their port facilities. However, once a national identity standard is promulgated, it is critically important that these standards supersede state regulations. Thus, the MTD recommends that the Federal TWIC or MMD program preempt any state or local regulations covering identity cards for mariners. The entire purpose of an identification credential is to provide a universally recognized identity card and to assure a mariner access to vessels and port facilities. In addition, the mandatory provisions of the International Maritime Organization's ISPS Code require facilitation of access by mariners. Additional state or local requirements will create confusion and intolerable conditions for mariners, undermine the purpose of the TWIC, and disrupt interstate and foreign waterborne commerce. Allowing states to arbitrarily impose different or added security requirements is inconsistent with the intent of the TSA to achieve a level of consistency governing threat assessments and transportation credentials.

Additional Comments on the TWIC Program

The MTD believes that the TWIC program, as explained in its final rule, will cause many unnecessary problems within the maritime industry, including potentially severe disruption to the livelihoods of mariners and other transportation workers who pose no threat to security and who have done nothing wrong. It will not enhance security but will certainly disrupt commerce and place an intolerable burden on American merchant mariners. The program is also flawed since it exempts foreign seamen from the process while focusing completely on U.S. merchant mariners who are screened, regulated and fully vetted by the Coast Guard. It has been estimated that 97 percent of our imports and exports are carried on foreign-flag vessels with foreign crews who in our view pose the gravest security risk. Yet, these crews are exempt from the TWIC requirements. In addition to our recommendations mentioned above, the MTD also advocates:

- That any national TWIC issued to American merchant mariners must be compatible with the International Labor Organization's Convention 185 (Seafarers Identity Document) so that there will be a consistency between national and international identity credentials.
- By the nature of their employment, mariners require access to secure areas throughout a port, a state, or even internationally. If mariners are required to obtain a TWIC, they should be guaranteed unfettered access to ports.
- There must be a clear nexus between terrorism security and the crimes that will disqualify an individual from holding a maritime TWIC, as the list of felony

offenses that will disqualify a mariner from obtaining a maritime TWIC is too expansive, nebulous and unfocused on eliminating true security risks. Although some modifications were made in the final rule to the original list of disqualifying offenses, the MTD urges the TSA to exercise appropriate discretion to not deny employment opportunities to those mariners who may have simply made a mistake years ago.

U.S. mariners are and will always be an effective asset in the global war on terrorism. They are the best trained, most qualified and most thoroughly vetted workers in the transportation industry. The U.S. Merchant Marine's history of answering the call to perform our patriotic duty in every conflict and disaster is a matter of public record. In summary and to be clear, we urge the TSA to recognize the contributions of American mariners to the economic and defense security of our Nation by exempting them from the unnecessary burden of obtaining a TWIC.

The MTD remains ready to work cooperatively with the Committee, the Transportation Security Administration and the Coast Guard to identify and implement the most fair and effective systems that promote security in the domestic maritime transportation network.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO HON. EDMUND S. "KIP" HAWLEY

Question 1. When will the Department provide Congress with the comprehensive management plan for TWIC that was required in the Intelligence Reform Act of 2004 and is over 2 years past due?

Answer. The Transportation Worker Identification Credential Program Management Plan, as required by the Intelligence Reform and Terrorism Prevention Act of 2004, is currently undergoing executive level review and clearance within the Department. The Transportation Security Administration anticipates delivery to Congress in the third quarter of the current fiscal year.

Question 2. Of the 4,000 TWIC cards you reported issued in the prototype testing, how many were activated? Of those activated how many were actually tested with a biometric card reader? Were any tested on vessels?

Answer. The Transportation Security Administration issued 4,362 cards during the prototype, all of which were activated. While we do not have data on how many of the activated cards were used in biometric readers, 3,209 biometric access attempts were made during the prototype phase. No readers were tested on vessels during the prototype phase.

Question 3. What vessel operators have you and the Coast Guard identified for participation in the card reader pilot mandated in the SAFE Port Act? How many vessels and over what duration of time do you plan on testing the technology?

Answer. The Transportation Security Administration (TSA) plans to test contactless biometric authentication technology that meets the requirements of the Transportation Worker Identification Credential (TWIC) reader specification in a variety of maritime operational scenarios (container, bulk, petroleum, and passenger terminals; and vessels), as well as in different geographic regions and climates. The final reader specification is pending a review of comments received from the public notice of the specifications recommended by the National Maritime Security Advisory Committee. The TWIC program, with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. Planning for this project has been underway since December 2006.

TSA is reviewing potential participants for the upcoming card reader pilot tests but they have not yet been finalized. Discussions are ongoing with the Ports of Los Angeles and Long Beach as well as the Ports of New York and New Jersey to identify vessel participants to include small passenger vessels and ferries. We are also working with the American Waterways Operators Association to identify an appropriate participant for the towboat and tug boat industry. The duration of the pilot tests will be such that the card readers will be tested under various environmental and operational conditions, although the duration has not yet been finalized.

Question 4. You mention in your testimony that the TSA has "created a new process where the TSA can make a determination that a security threat assessment conducted by another government agency is comparable, eliminating redundancy and reducing costs for workers." Can you describe this?

Answer. The Transportation Security Administration (TSA) may determine that security threat assessments conducted by other governmental agencies are comparable to the Transportation Worker Identification Credential/Hazardous Materials

Endorsement threat assessment. In making a comparability determination, TSA will consider (1) the minimum standards used for the security threat assessment; (2) the frequency of the threat assessment; (3) the date of the most recent threat assessment; and 4) whether the threat assessment includes biometric identification and a biometric credential. The procedures to apply for a comparability determination are outlined in 49 CFR § 1572.5(e) Comparability of Other Security Threat Assessment Standards. TSA will notify the public by publishing a Notice in the *Federal Register* when a comparability determination is made.

Question 5. Have you reached out to other agencies such as the Department of Defense and the Department of Energy to determine what background check and credentialing process they have in place and how are they comparable to TSA's background checks for TWIC? What credentialing programs have you found to be comparable to other Federal agencies' programs?

Answer. The Transportation Security Administration discussed comparability with both the Department of Defense (DOD) and the Department of Energy. DOD is gathering the information needed in order to make a comparability determination. Thus far, the background checks performed by U.S. Customs and Border Protection for the Free and Secure Trade program, and the U.S. Coast Guard for the Merchant Mariner Document program, have been determined to be comparable to that of the Transportation Worker Identification Credential.

Question 6. I understand you have developed procedures to reduce the TWIC fee for transportation worker that have had comparable background checks, such as the Hazardous Materials Endorsement (HME) and the Merchant Mariner Document (MMD). However, what procedures have you put in place to ensure that individuals who have received a TWIC do not have to undergo and pay for redundant background checks when applying for a HME or MMD?

Answer. The Hazardous Materials Endorsement (HME) process, fee structure, and contract vehicles were implemented in January 2005 to meet the requirements of the USA PATRIOT Act of 2001 (Public Law 107–56). Presently there is no mechanism or ability to reduce this redundancy for HME drivers within the confines of the present fee rule and contractual vehicles. The Transportation Security Administration is in the process of developing a new fee rule, as well as a new acquisition, that will take this issue into account and will more fully align the HME check, as well as future threat assessment programs, with that of the Transportation Worker Identification Credential. The intention is to reduce the burden on multiple credential holders to the greatest extent possible.

With respect to the MMD, TSA and Coast Guard are in discussions regarding the details of this issue. As you know Coast Guard is moving to a consolidated Merchant Mariner Card (MMC) and expects to recognize the TWIC as the identity document for merchant mariners. Coast Guard will not charge mariners a duplicative fee for the same requirement already fulfilled under TWIC.

Question 7. TSA originally expected TWIC enrollments to begin at the Port of Wilmington by March 28, 2007—the effective date of the TWIC rule. However, enrollments did not begin on this date as planned. What is the reason for the delay and when does TSA plan to begin enrolling workers at the port?

Answer. It is imperative that enrollments begin as soon as possible, and TSA is working diligently to that end. At the same time our highest priority is to ensure that the Transportation Worker Identification Credential (TWIC) enrollment and credential issuance process is as efficient and trouble-free for the first worker as for those who will follow. TSA expects to begin enrollment in the Fall of 2007, but that is subject to our ongoing, rigorous assessment of the TWIC system.

TWIC is a sophisticated system powered by state-of-the-art technologies and we are focused on a rigorous program to "flight test" TWIC before it is rolled out to the ports.

The TWIC network includes technology components covering five important areas:

- The Pre-Enrollment website component allows workers to schedule appointments and provide biographic information ahead of time to make enrollment easier.
- The Enrollment workstation component captures a worker's biometric and biographic information and submits the information for completing the Security Threat Assessment (STA).
- The TWIC system includes components that route applicant information for the STA, store data, conduct data integrity checks, and manage status on TWIC cards.

- The Screening Gateway component is a TSA enterprise asset that facilitates STA's, working with the Federal Bureau of Investigation, Citizenship and Immigration Services, and TSA's Colorado Springs Operations Center.
- Finally, the Card Production component electronically loads an applicant's information onto a TWIC smart card and then physically produces the card.

All the internal moving parts must work together, to conduct accurate and timely security threat assessments. We recognize that TWIC will affect both businesses and port workers and a top priority is making sure the program does not negatively impact commerce or people's livelihoods.

Question 8. How does TSA plan to meet the requirement of the SAFE Port Act that TWIC be implemented at the 10 highest risk ports by July 1, 2007? How does TSA interpret the term "implemented" in this requirement? What challenges do TSA and Lockheed Martin face in meeting this and other time frames in the Act? When does TSA plan to set specific dates requiring TWIC to be used at specific ports?

Answer. It is imperative that enrollments begin as soon as possible, and TSA is working diligently to that end. At the same time our highest priority is to ensure that the Transportation Worker Identification Credential (TWIC) enrollment and credential issuance process is as efficient and trouble-free for the first worker as for those who will follow. TSA expects to begin enrollment in the Fall of 2007, but that is subject to our ongoing, rigorous assessment of the TWIC system. Our highest priority is to ensure that the Transportation Worker Identification Credential (TWIC) enrollment and credential issuance process is as efficient and trouble-free for the first worker as for those that follow. It is our intention to meet the remaining deadlines set forth in the SAFE Port Act. The Coast Guard will establish compliance dates by Captain of the Port zones after the base population has been enrolled and received their TWICs. This date will be published in the *Federal Register* at least ninety days before compliance is required in each Captain of the Port zone.

Question 9. What oversight mechanisms is TSA using to ensure that all requirements of the TWIC enrollment contract are met? What specific steps does TSA plan to take to verify contract performance data provided by Lockheed Martin?

Answer. The current contract is performance based with a defined Quality Assurance Surveillance Plan with defined Acceptable Quality Levels (AQLs). An award fee structure is also in place to provide incentives for improved performance as well as disincentives should the contractor not meet the AQLs. Performance Management Reviews are being conducted monthly. In addition, there will be periodic site visits to enrollment centers to validate and verify reported performance data. As a further oversight measure, TSA has engaged an IV&V contractor to review technical deliverables. TSA plans to continue the IV&V contract as the program moves forward.

Question 10. Mr. Hawley's statement indicates that the Lockheed Martin contract requires adaptive planning, metrics, and changes. Can you please explain what you mean by this statement?

Answer. Lockheed Martin is contractually required to support the enrollment of the Transportation Worker Identification Credential population nationwide. To satisfy this requirement Lockheed Martin has developed a flexible deployment strategy to take into account the need to respond to enrollment surges, a mobile population, and enrollment facility options. The contract clearly defines Acceptable Quality Levels within the Quality Assurance Surveillance Plan with which Lockheed Martin must adhere. The contract vehicle provides the Transportation Security Administration with the flexibility to add enrollment capability as the program is implemented.

Question 11. When does TSA plan to begin the pilot program to test TWIC access control technologies? What specific technologies does TSA plan to test during the pilot?

Answer. The first two pilot locations have been awarded grant funding—Ports of LA (POLA) and Long Beach (POLB). Additional locations will be selected from the grantees in the latest round of Port Security Grants. We have finalized the cooperative agreement with POLB, POLA will finalize shortly. We are developing the comprehensive test and evaluation plan and expect POLA and POLB to begin working with terminal operators to identify the right locations for TWIC readers and start taking metrics for currents operations.

The actual readers will begin testing after finalization of the contactless biometric authentication specification that will be used has been published, and industry has developed the necessary card reader equipment. Planning for this project has been underway since December 2006.

TSA plans to test contactless biometric authentication technology that meets the requirements of the TWIC reader specification in a variety of maritime operational scenarios (container, bulk, petroleum, and passenger terminals; and vessels), as well as in different geographic regions and climates. The program has been working with other DHS entities (S&T Directorate, USCG, G&T, SCO) and the National Institute of Standards and Technology to develop the tests to assure baseline performance for this technology. TSA is also collaborating with the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

Question 12. Does TSA plan to measure the impact that the TWIC program will have on the flow of maritime commerce during the pilot program? If so, how does TSA plan to do this? How will TSA ensure effective communication and coordination with maritime industry stakeholders during implementation of TWIC?

Answer. Obtaining current "as is" state and comparing that to the "to be" state utilizing Transportation Worker Identification Credential (TWIC) card readers is the primary focus of the pilot. The pilot Test and Evaluation Master Plan (TEMP) will address areas to be tested, required metrics, and test responsibilities. The Transportation Security Administration anticipates completing the TEMP this summer. Stakeholders will continue to be apprised of the deployment status through regular meetings of the TWIC Stakeholder Communications Committee (TSCC) and our participation in various conferences, meetings, and briefings. The TSCC is comprised of stakeholder representatives from labor, ports, vessels, and other industries that will be impacted by TWIC.

Question 13. What steps are TSA and Lockheed Martin taking to identify the entire population affected by the TWIC rule and educate this population on their responsibilities for enrolling in the TWIC program?

Answer. The Transportation Security Administration (TSA) and Lockheed Martin have implemented a robust, multi-faceted outreach and communications process to identify and educate the population affected by the Transportation Worker Identification Credential (TWIC). This strategy includes regular meetings of the TWIC Stakeholder Communications Committee comprised of stakeholder representatives from labor, ports, vessels, and other industries that will be impacted by TWIC and a Lockheed Martin TWIC field organization that is in contact with local Coast Guard Captains of the Port, Port Authorities, major port officials, industry, and labor representatives.

The Transportation Security Administration and the Coast Guard are also leveraging their extensive relationships with affected stakeholders from both industry and labor that have been developed over years of cooperation in the transportation sector.

Question 14. Why did the TSA and the Coast Guard reject adopting the International Civil Aviation Organization (ICAO) standard? Will the TWIC be designed to be interoperable with the ICAO standard? If no, why?

Answer. In developing the Transportation Worker Identification Credential (TWIC), the Transportation Security Administration considered a wide variety of document standards. The starting point is the program's requirements and fundamentally TWIC was developed as a secure identity document for physical access, pursuant to Congressional mandates. It is not a travel document that would be recognized internationally.

It is important that credentials issued to U.S. Federal standards be interoperable with the TWIC and across the U.S. transportation system. Therefore, to achieve maximum interoperability with other programs, TWIC follows Federal Government standards for biometric credentials which are contained in Federal Information Processing Standard 201 (FIPS 201) and the underlying Federal standard for Minutia fingerprint templates contained in the American National Standards Institute publication 378. The industry expects the FIPS 201 standard to be the primary standard across such operations into the future.

Question 15. What assurance does TSA have that the agency is prepared to handle the volume of workers that may appeal the result of the threat assessment or those that may request a waiver if they do not meet the eligibility requirements?

Answer. The Transportation Security Administration (TSA) is leveraging time-tested processes and procedures that have been developed and implemented successfully in programs such as the Hazmat Threat Assessment Program. In the Hazmat program, security threat assessments are conducted on commercial truck drivers seeking to obtain, renew, or transfer a hazardous materials endorsement on their state issued commercial driver's license. The Hazmat program has been operating successfully since January 2005 and has received over 550,000 applications via a nationwide system of TSA contracted enrollment stations and state licensing agencies. TSA has received waiver and appeal requests on approximately 1.5 percent of this

population. The standard operating procedures and policies for adjudications and redress have been proven successful. TSA has an existing contract in place to support adjudications including the waiver and appeal process. This contract is scalable and can surge to meet the demands of TWIC.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TED STEVENS TO HON. EDMUND S. "KIP" HAWLEY

Question. Millions of dollars have been spent and multiple delays have been experienced with the Transportation Security Administration's (TSA) Registered Traveler (RT), Secure Flight, and Transportation Worker Identification Credential (TWIC) programs. Should TSA follow the path it took with RT and allow the private sector to run these programs? What assurances can you give that TSA will be able to execute and sustain these types of programs?

Answer. While there are significant differences in the statutory language mandating the Transportation Worker Identification Credential (TWIC) and Secure Flight and the language and intent concerning Registered Traveler (RT) the Transportation Security Administration (TSA) believes that all three programs cannot be implemented without significant input from the private sector.

In the case of RT, TSA was provided broad discretion to design and implement the program. The RT Interoperability Pilot was designed to test the public-private partnership and to encourage innovation in the market place. At the same time, there are certain program activities that are inherently governmental. TSA directly administers those functions, such as setting program security and compliance standards and completing the security threat assessment on RT applicants.

Unlike RT, the Secure Flight and the TWIC programs are based on specific legislative mandates. For Secure Flight, TSA has been directed to assume the watch list matching currently performed by aircraft operators. Furthermore, the Maritime Transportation Security Act as amended by the SAFE Port Act requires the Secretary of Homeland Security to issue a biometric credential (TWIC) and conduct security threat assessments on individuals who have unescorted access to secure areas of maritime facilities and vessels. As a result, Secure Flight and TWIC are centrally managed by the Federal Government to assure security, privacy, interoperability, and enforcement.

Nevertheless, TSA has sought significant input from the private sector to develop these programs. For TWIC, TSA has requested the National Maritime Security Advisory Committee, with representation from the stakeholder community and credential reader manufacturers, to recommend standards for use for a contactless credential reading solution. Secure Flight is being developed with direct input from the airline industry and is responding directly to requests for a single DHS interface to air carriers.

TSA recognizes that both programs have faced tremendous challenges in moving toward implementation. Both involve significant IT investments and strong program management. TSA has taken steps to address critical program management requirements, instilling discipline into the process for both TWIC and Secure Flight, and is positioning itself to execute and sustain these programs.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO HON. EDMUND S. "KIP" HAWLEY

Question 1. How many workers nationwide are expected to need TWIC cards? Can you tell me what estimates TSA intends to use for the number of workers requiring TWIC cards at the Port of New York and New Jersey, and whether sufficient resources will be available to provide these cards in a timely and efficient way?

Answer. The Transportation Security Administration estimated 750,000 transportation workers would require Transportation Worker Identification Credentials (TWICs) to meet the mandates of the Maritime Transportation Security Act of 2002. Of that total, approximately 60,000 were estimated to be within the Port Authority of New York and New Jersey. The TWIC contractor is responsible for ensuring sufficient resources are in place to conduct timely and efficient enrollments and card issuance during the initial enrollment period. The contractor has flexibility to add or re-adjust assets as required to ensure adequate resources are in place to provide these cards in a timely and efficient manner.

Question 1a. Is the number of enrollment stations based upon the affected population estimates published in the TWIC final rule? When will you and the contractor determine where the estimated 130 enrollment centers will be located?

Answer. The number of enrollment workstations in each port is based on a number of factors including the population estimate for that port, the geographic size of the port, and the duration of the initial enrollment period for that port. The Transportation Worker Identification Credential contractor, in cooperation with the Transportation Security Administration and the Coast Guard, is in the process of evaluating each port to determine the number and location of enrollment sites.

Question 1b. What steps do you plan to take if your population estimates are found to be too conservative?

Answer. The Transportation Security Administration, the Coast Guard, and the Transportation Worker Identification Credential (TWIC) contractor will continue to communicate with local stakeholders and monitor the enrollment population to ensure adequate resources are deployed to enroll the affected population in an effective manner. The TWIC contractor is responsible for ensuring sufficient resources are in place to conduct timely and efficient enrollments and card issuance during the initial enrollment period. The contractor has the flexibility to add or re-adjust assets as required to ensure adequate resources are in place to provide these cards in a timely and efficient manner.

Additionally, the TWIC contract contains a Quality Assurance Surveillance Plan with Acceptable Quality Levels for enrollment and wait times against which the contractor will be measured.

Question 1c. If population estimates are considered too conservative, will TSA be required to modify the contract with Lockheed Martin?

Answer. Modifications to the contract should not be required. The Transportation Worker Identification Credential contract is performance based and the prime contractor receives a portion of the user fee for each transaction. Included in the contract are award incentives for the contractor to exceed enrollment projections.

Question 2. Given that a transportation worker has to appear at an enrollment center at least two times (enrollment and card issuance), how is the TSA going to ensure the level of staffing and processing times (15 minute processing) are sufficient to minimize the impact on industry and the flow of commerce?

Answer. The Transportation Security Administration will monitor the contractor's performance through site visits, customer surveys, and program management reviews. The Transportation Worker Identification Credential contract includes incentive and disincentive provisions for contractor performance. The processing time, which is highly dependent on the contractor's staffing level, will be a significant factor in the contractor performance evaluation. Also, the system incorporates a pre-enrollment website component that allows workers to schedule appointments and provide biographic information ahead of time to make the enrollment process more efficient.

Question 3. If the initial enrollment is expected to take an extended period of time in a particular port (*i.e.,* 9–12 months in NY/NJ), how are the TSA and the USCG going to ensure that transportation workers avail themselves to the enrollment process throughout the entire period? Inevitably many people will put off their enrollment until shortly before the enforcement date. How is the contractor going to handle the surge in volume that is expected 30 days prior to enforcement in a given port?

Answer. The Transportation Security Administration, the Coast Guard, and the Transportation Worker Identification Credential (TWIC) contractor are working to develop effective outreach and communications with stakeholders, including employers, unions, and advocacy groups, to generate a steady flow of enrollment throughout the enrollment period. The TWIC contractor is responsible for ensuring sufficient resources are in place to conduct timely and efficient enrollments and card issuance during the initial enrollment period. The contractor has the flexibility to add or re-adjust assets as required to ensure adequate resources are in place to provide these cards in a timely and efficient manner. Additionally, the TWIC contract includes award incentives for the contractor to exceed enrollment projections. Some responsibility, however, must still fall on facilities, employers, and the transportation workers themselves to enroll in time to ensure they can be eligible for unescorted access to secure areas before the compliance date established for each port.

Question 4. It is my understanding that TSA has suggested taking resources from the Port Security Grant program to pay for the TWIC pilot project. Why didn't the President's request separate funding for the pilot project?

Answer. Terminal and vessel operators are responsible for access control into their facilities. The use of Port Security Grant funds for the purchase of card readers and associated infrastructure to conduct the pilot test is appropriate since the terminal and vessel operators will be able to keep the equipment and access control

system improvements to comply with the Transportation Worker Identification Credential reader rule once it is effective. In addition, much of the work conducted through the test would have to be completed by the ports and facilities or vessels at their locations, in order to implement the TWIC reader requirements. We also believe that this use increases the overall level of security measures in place.

Question 5. I don't expect this TWIC program to be completed anytime soon. In the meantime, when will you complete the terror watch-list checks for port truck drivers, as you were required to do in the SAFE Port Act, and as you have done for other workers with access to secure areas of ports? Has FMCSA provided a complete list of Commercial Drivers License holders to you? If not, how will you proceed?

Answer. The Transportation Security Administration (TSA) intends to meet these requirements through Transportation Worker Identification Credential (TWIC) enrollments and security threat assessments which will begin at the conclusion of our TWIC system performance testing. TWIC implementation will capture this information and make the vetting process go smoothly without the need to undertake a second rulemaking.

Section 125 of the Security and Accountability for Every Port Act (Public Law 109–347) addresses a population on which no government entity, association, or industry organization maintains information. Generally, each port Terminal Operator has contracts with a number of transportation companies that provide drivers and trucks to transport containers from secure areas to staging areas. Neither the Terminal Operator nor the trucking companies know which drivers may enter a port on any given day or at all. Most trucking companies do not have all of the information necessary to successfully complete the vetting on each of their drivers to submit to TSA. There are over 500,000 trucking companies, many of which are independently owned and operated and tend to move to where the business is with no single company affiliation.

Question 6. In a joint USCG/TSA Notice of Proposed Rulemaking that was published in May 2006, a contact reader with pin technology was proposed. Industry vehemently opposed this technology solution because of the negative impact it would have on terminal efficiency. Where does the TSA now stand on this issue?

Answer. Based on comments received during the Notice of Proposed Rulemaking process the Transportation Security Administration (TSA) bifurcated the rule. The first rule that was published in the *Federal Register* on January 25, 2007, does not impose the requirement on owners/operators to purchase, install, or maintain card readers. A second rulemaking will address the card readers. The public will have ample opportunity to comment on this second rulemaking. TSA and the Coast Guard will consider all comments when determining what technology or processes are required to ensure that security of information and privacy is protected, as well as operational efficiency, in developing a final technology solution.

In March 2007, the U.S. Coast Guard invited public comment on a draft Transportation Worker Identification Credential (TWIC) biometric reader specification and a draft TWIC contactless smart cart application recommended by the National Maritime Security Advisory Committee that did not require use of a PIN. The final reader specification is pending a review of comments received from the public notice. TSA then plans to test contactless biometric authentication technology that meets the requirements of the TWIC reader specification in a variety of maritime operational scenarios (container, bulk, petroleum, and passenger terminals; and vessels), as well as in different geographic regions and climates. TSA, with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

Question 7. The SAFE Port Act requires the TSA to establish a pilot program to test the card reader technology at 5 geographically distinct port locations within 6 months of enactment. When and where will these pilot projects commence and how long are they funded?

Answer. The first two pilot locations have been awarded grant funding—Ports of LA (POLA) and Long Beach (POLB). Additional locations will be selected from the grantees in the latest round of Port Security Grants. We have finalized the cooperative agreement with POLB, POLA will finalize shortly. We are developing the comprehensive test and evaluation plan and expect POLA and POLB to begin working with terminal operators to identify the right locations for TWIC readers and start taking metrics for currents operations.

The actual readers will begin testing after finalization of the contactless biometric authentication specification that will be used has been published, and industry has developed the necessary card reader equipment. Planning for this project has been underway since December 2006.

TSA plans to test contactless biometric authentication technology that meets the requirements of the TWIC reader specification in a variety of maritime operational scenarios (container, bulk, petroleum, and passenger terminals; and vessels), as well as in different geographic regions and climates. The duration of the pilot tests will be such that the card readers will be tested under various environmental and operational conditions, although the duration has not yet been finalized.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO HON. EDMUND S. "KIP" HAWLEY

Question 1. While I appreciate TSA's willingness to further study the requirement directing each towing vessel to carry a card reader, I remain concerned about the effect of this requirement on the maritime industry, particularly its small businesses. As you know, there is significant opposition to requiring card readers on every towing vessel. Given that crew sizes on tug boats reportedly run between four and ten mariners, and each of those mariners is well known to other mariners on the tug, as well as management, therefore making any intruder obvious, do you believe a workable compromise could be reached, such as only requiring card readers on vessels employing ten or more mariners?

Answer. The Coast Guard will be evaluating and considering multiple types of operations and scenarios as the proposed requirements for the second Transportation Worker Identification Credential (TWIC) rule are developed. When determining reader applicability, crew size and vessel type are very likely to be considered in addition to risk.

Question 2. The TWIC application process remains burdensome on workers and the industries depending on them. Easier access to TWIC cards once granted may help relieve some of this burden without causing undue security concerns. Many are concerned about the cumbersome process to apply for a TWIC card, including the long distances some workers will be required to travel to obtain a TWIC card. This is especially true for those in the long haul trucking industry who may end up applying for their card at one enrollment center, but due to the nature of their employment may be far from that center by the time the card is ready. In your opinion, would allowing applicants to designate that cards be returned to a different enrollment center than where they originally applied or alternatively including a mechanism to mail cards to an applicant's home or office be realistic fixes for this problem? If not, what do you propose as an alternative?

Answer. Shipping a Transportation Worker Identification Credential to an enrollment center other than the one at which enrollment took place was considered during the planning stages of the program. Mailing cards directly to the applicant was also considered. To make system changes to accommodate these alternatives at this time would be costly and could further delay implementation. Mailing cards directly to the individual raised security concerns as the Transportation Security Administration (TSA) would not be able to ensure the individual receiving the card was in fact the individual that applied for the card. Although these methods were excluded as part of our original business plan, TSA may reconsider these options as experience is gained with the current system and processes in order to reduce the burden on the affected population.

Question 3. The costs associated with TWIC may be a barrier for some workers and businesses. While I understand those costs may compare favorably with other card fees, they remain a burden for the temporary, seasonal labor in the maritime industry. Of particular concern is the fact that an applicant must pay for the full price of the application up front, leaving those applicants who are denied cards paying for the production of cards they do not receive. One potential solution may be not to reduce the overall costs, but the schedule on which they are paid. In your opinion, would it be possible for TSA to charge only for the cost of processing the application and the security assessment up front, with the balance to be paid should a card be granted?

Answer. The Transportation Security Administration (TSA) believes the current process of payment and fee collection provides the best value to the total population and limits the overall cost of the credential. While workers ultimately denied a Transportation Worker Identification Credential (TWIC) may pay for the card production and issuance portion of program costs, they benefit from having all applicants sharing equally in the cost of the process. Workers whose criminal history

would otherwise result in denial of a TWIC may request a waiver through the TSA redress process and review by an administrative law judge. Adopting a position that TWIC applicants should only pay for the services they directly receive could result in considerable costs to those applicants utilizing the redress process.

Question 4. The goal of the TWIC program is to strengthen the security of our transportation system, starting with the implementation of a pilot without unintended consequences. Unfortunately, a host of issues have plagued the successful implementation of the pilot, including an incomplete management plan to date, lack of contract accountability, and ever-increasing costs to implement the program. I am concerned that if we don't fix these problems soon, we jeopardize the health of our workforce, strength of our economy, and overall, security of our Nation. Given these are just some of the implementation issues since the TWIC pilot was first authorized in 2001, please describe how our workforce and economy has been indirectly impacted by these delays.

Answer. The Transportation Worker Identification Credential (TWIC) is only going to improve what is currently a less than ideal situation in the maritime sector of our Nation's transportation system. The maritime workforce does not currently have a common, secure, interoperable credential that can be used for nationwide access to maritime facilities, as the TWIC is intended to provide. Workers may be required to purchase multiple credentials and undergo multiple background checks to gain access to facilities sometimes even within the same state. The intent of the TWIC is to provide this capability in the form of a uniform identity credential based on a minimum Federal security standard and centralized processes that can replace the many credentials that may be required today.

Question 5. It is my understanding that the TWIC system will not be interoperable with international standards. I am concerned that without uniformity of international standards, non-U.S. crewman will be exempt from complying with our security provisions when entering U.S. ports. Do you think it is necessary to establish an uniform international ID standard? What is the agency's plan to sync the TWIC system with the current biometric technology used by the United Nations and developed by the International Civil Aviation Organization (ICAO)?

Answer. Obtaining current "as is" state and comparing that to the "to be" state utilizing Transportation Worker Identification Credential (TWIC) card readers is the primary focus of the pilot. The pilot Test and Evaluation Master Plan (TEMP) will address areas to be tested, required metrics, and test responsibilities. The Transportation Security Administration anticipates completing the TEMP this summer. Stakeholders will continue to be apprised of the deployment status through regular meetings of the TWIC Stakeholder Communications Committee (TSCC) and our participation in various conferences, meetings, and briefings. The TSCC is comprised of stakeholder representatives from labor, ports, vessels, and other industries that will be impacted by TWIC.

The United Nations through the International Labor Organization developed a seafarer credential with the intention of endorsing it as a universally recognized visa. The U.S. supports the concept of raising the level of seafarer document security but continues to have some concerns about the ILO document. TSA will continue to monitor international developments and protocols to determine what, if any, benefits to the program they provide.

Question 6. The enrollment of workers at the Port of Seattle was scheduled to begin on March 26. When and by what means did TSA notify the Port that the March 26 date would slip? What effort will TSA make to ensure the Port's management is fully informed of the new schedule for TWIC enrollment when it becomes available?

Has the TWIC contractor physically established a TWIC enrollment center for the Port of Seattle? The Port estimates that approximately 100,000 individuals will require a TWIC. How many enrollment agents does the contractor intend to hire to handle the number of individuals that will have to be enrolled?

Answer. The Transportation Security Administration (TSA) has not published an official enrollment schedule and has not notified the Port of Seattle when enrollments will commence at that location. TSA and Lockheed Martin commenced a robust, multi-faceted outreach and communications process to identify and educate the population affected by the Transportation Worker Identification Credential (TWIC). This strategy includes regular meetings of the TWIC Stakeholder Communications Committee comprised of stakeholder representatives from labor, ports, vessels, and other industries that will be impacted by TWIC and a Lockheed Martin TWIC field organization that is in contact with local Coast Guard Captains of the Port, Port Authorities, major ports officials, industry, and labor representatives. Once TSA de-

termines we are prepared to begin issuing notice on enrollment, this outreach effort will expand significantly.

Lockheed Martin has met with Seattle maritime officials; however, specific Seattle enrollment sites have not been established. Lockheed Martin is contractually required to support the enrollment of the TWIC population nationwide. In order for them to satisfy this requirement Lockheed Martin has developed a flexible deployment strategy to take into account the need to respond to enrollment surges, a mobile population, and enrollment facility options. The contract clearly defines Acceptable Quality Levels within the Quality Assurance Surveillance Plan to which Lockheed Martin must adhere. The contract vehicle provides TSA with the flexibility to add enrollment capability as the program is implemented.

Question 7. The SAFE Port Act requires TSA to conduct a pilot program to test the business process, technological, and operational impacts of TWIC deployment at not fewer than five distinct geographic locations and to include vessels and facilities in these tests. What is the status of these pilot programs and the required testing?

Answer. Planning for the pilot programs has been underway since December 2006. A pilot test agreement has been reached with the Port of Long Beach and approval of an agreement with the Port of Los Angeles is expected in the next few months. Discussions are also ongoing with the Port Authority of New York and New Jersey to finalize their participation. TSA, with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

Question 7a. When and where will the first full scale pilot program testing of an automated TWIC system be?

Answer. The first Early Operational Assessment test will be conducted in conjunction with the Ports of LA and Long Beach this year.

Question 7b. My understanding is that some early testing of TWIC prototypes was conducted at the ports in Washington. Will TSA be conducting any further testing of TWIC at these ports prior to requiring full deployment?

Answer. The Transportation Worker Identification Credential prototype tests were conducted in three geographic areas: Los Angeles and Long Beach; Delaware River Basin; and Florida.

Question 7c. Has TSA determined all five locations that will be used for testing? If not, when do you expect to do so?

Answer. The first two pilot locations have been awarded grant funding—Ports of LA (POLA) and Long Beach (POLB). Additional locations will be selected from the grantees in the latest round of Port Security Grants. Discussions are also ongoing with the Port Authority of New York and New Jersey to finalize their participation and we are working with the American Waterways Operators Association to identify an appropriate participant for the towboat and tug boat industry.

Question 7d. What is the required error rate for the TWIC card? Can you please describe the scope and methodology that will be used to test the error rate of the TWIC card?

Answer. The Transportation Worker Identification Credential will be aligned with the Federal standards for government credentials contained in the National Institute of Standards and Technology's (NIST's) Federal Information Process Standard 201–1 and associated standards such as those in NIST's Special Publication 800–76. 800–76 specifies a false rejection rate (FRR) of less than or equal to 1 percent and a false acceptance rate (FAR) of 1 percent. The FRR is the percentage of incorrectly rejected valid users. The FAR is the percentage of imposters incorrectly matched to a valid user's biometric.

The Transportation Security Administration (TSA), with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

Question 7e. Were private sector representatives, such as terminal and vessel operators, included in developing the scope and methodology for this testing?

Answer. TSA has used comments provided in response to the TWIC NPRM published in May 2006 as well as its work with the National Maritime Security Advi-

sory Committee in developing the scope of the pilot tests. We are working with the Ports of LA and Long Beach and will work with the other pilot locations as well to incorporate their feedback. Specifically to testing parameters, the Transportation Security Administration (TSA), with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing. TSA will, at the appropriate time, seek operator input as the test plans are developed to ensure full participation from stakeholders and a robust meaningful pilot test is conducted.

Question 8. Your agency, along with the Coast Guard, has requested comments on the TWIC technology specification recommendations developed by the National Maritime Security Advisory Committee (NMSAC). I understand that those comments where due on March 30 of this year. Can you give the Committee a general overview of the comments received?

Answer. Over thirty separate entities submitted comments to the questions posed in the Transportation Worker Identification Credential (TWIC) Contactless Biometrics Specification Public Notice published in the *Federal Register*. Entities were predominantly from the maritime community and its trade associations but some represented technology companies and technology trade associations. Generally the commenters praised the work of the National Maritime Security Advisory Committee (NMSAC) TWIC Contactless Specification Workgroup.

Commenters also generally agreed that a PIN was not a good idea for general use due to operational concerns. Others believe the PIN should be considered only if it can be shown not to affect operations. A number of commenters believe the impact of lost PINs would be burdensome to the TWIC users and to the program.

Most commenters agreed that privacy was important but most in the maritime industry did not have concerns that any measures were required to protect the privacy of biometric fingerprint templates. On the other hand, most in the technology industry believe that biometric fingerprint templates should be protected, but that the TWIC Privacy Key (TPK) scheme is sufficient to protect the template.

A number of maritime commenters carried forward their concerns about PINs, encryption of fingerprint biometric templates and use of the TPK card magnetic stripe swipe concept as having potential negative impact on port and facility operations. Commenters also mentioned that the pilot tests would be useful for identifying impacts on facility and vessel operations. Specifically, commenters were concerned about error rates that might impact gate throughput, operation during extreme situations, allowing cleaning and vending personnel into facilities without a TWIC, the effect of TWIC at various Marine Security levels.

Commenters generally agreed that TWIC would have a large impact on currently deployed personnel access control systems (PACS) if they were to be integrated and duplicative if they are not.

A number of commenters reiterated their endorsement of the NMSAC recommendation as being the one that would have minimal impact on the cost of port security operations. Commenters with PACS were concerned with integrating TWIC into their operation, especially the impact of the recommendation that includes encryption of biometrics and possible need of wiring upgrades. Commenters were interested in impacts on both acquisition/installation and operational costs. Commenters without current PACS were concerned that TWIC would require PACS to be procured, installed, and maintained.

Almost universally commenters agreed that a Qualified Products List should be developed.

Question 8a. When do you expect to complete a review of the requested comments and provide a proposed rule on the technology that will be required to be deployed at our Nation's port to support the TWIC?

Answer. The Transportation Security Administration's goal is to publish the final specification within the coming months. The Transportation Worker Identification Credential rule requiring readers will follow the notice and comment rulemaking process after initial pilot test results have been collected and reviewed.

Question 8b. How is the development and deployment of the technology behind TWIC being coordinated with the testing required by the SAFE Port Act?

Answer. The pilot tests TSA is planning pursuant to the SAFE Port Act, will inform the follow-on rulemaking to require deployment of TWIC readers. The Transportation Security Administration (TSA), with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation

Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

Question 8c. When do you expect to publish a final rule on the technology of TWIC technology and will it be published before your agency completes the testing?

Answer. The Transportation Worker Identification Credential (TWIC) rule requiring readers will follow the Notice of Proposed Rulemaking (NPRM) process after initial pilot test results have been collected and reviewed. The Coast Guard and the Transportation Security Administration have begun work on the TWIC II NPRM and expect to publish it in early 2008.

Question 9. Regarding the testing at the Ports of Los Angeles and Long Beach: I understand that the Ports where awarded Maritime Security Grants to help cover the cost of testing and implementation. These grants in general, require the ports to provide matching state and local funding in the amount of 25 percent. I am told that your agency is requiring the full 25 percent match in the case of both testing and implementation. Do you agree that the development and testing of the TWIC technology standards is a Federal security responsibility? If not, why not?

Answer. Yes, although the Transportation Security Administration has sought, and continues to seek, input from affected industry stakeholders to ensure security goals are achieved while minimizing the effect on commerce and people. In addition, the pilot test TSA is conducting pursuant to the SAFE Port Act will facilitate implementation at the participating locations. As such, they are critical partners.

Question 9a. Can you explain the reasoning behind requiring select state and local governments to match Federal funding for testing a system that will be deployed nationwide?

Answer. Federal funding provides for equipment and infrastructure improvements that will remain in place during and after the Transportation Worker Identification Credential (TWIC) pilot test has concluded and will facilitate compliance with the TWIC card reader rule. Therefore, it is appropriate for owners and operators to fund a portion of the infrastructure.

Question 9b. Will your agency be requiring the other ports at which you will be conducting pilot program testing to provide matching funding for the testing phase?

Answer. Yes, all ports that participate in the pilot program using grant funding will be required to provide matching funds pursuant to the grant guidance.

Question 9c. How much total funding are state and local governments going to be expected to pay for testing the purposed TWIC technology?

Answer. The total amount of funds expended by state and local governments will depend on the amount awarded and utilized for equipment and infrastructure improvements by those ports and facilities participating in the test.

Question 9d. What happens if the testing proves the system that is developed does not work? Will you reimburse state and local governments for the money they contributed to testing?

Answer. The fingerprint template biometric technology that will be used by Transportation Worker Identification Credential (TWIC) has been extensively tested both by the biometrics industry and the Federal Government (National Institute of Standards and Technology and General Services Administration) and is in use in numerous applications. The primary question to be answered by the pilot test is not whether this technology works, but what the impact of requiring its use in the maritime industry will be where current regulations only require a visual inspection of identification. As noted above, facilities will be the beneficiaries of equipment purchases and infrastructure improvements; therefore, there are no plans to reimburse participants for funds expended for this purpose.

Question 9e. What alternatives, such as public-private partnership have you explored to get testing completed in a timely manner?

Answer. The Transportation Worker Identification Credential pilot testing, and the specification development preceding the pilot test, is an example of a public-private partnership. The contactless specification published for public comment was recommended by the National Maritime Security Advisory Committee working group in partnership with the Transportation Security Administration and the Coast Guard. Pilot test plans will be developed with input from the volunteer participants.

Question 10. I understand that the terminal operators at the Ports of Los Angeles and Long Beach already maintain a database of over 9,000 transportation workers (mostly truckers) that regularly call on the terminals and require unescorted access.

Have you considered using this existing database as a way to move forward with testing technology before prior to completing registration of port and transportation workers? If so, where does this effort stand? If not, why not?

Answer. The Transportation Security Administration (TSA) will consider all options for pilot testing within the parameters of its Testing and Evaluation Master Plan. TSA intends to conduct end-to-end testing of the Transportation Worker Identification Credential (TWIC) system and it is unlikely an existing database contains the fingerprints needed to create the fingerprint template for use in biometric matching. Additionally, during prototype testing, TSA attempted to use existing databases of maritime workers to expedite enrollment with unsatisfactory results. The databases contained data element errors (nick-names instead of given names, out of date address and phone information, no audit trail of identification verification, among others) and technical errors in formatting that were difficult to identify and resolve. TSA has no plans to rely on other databases for enrollment information for actual TWICs or to issue test credentials.

Question 11. The ports in my State of Washington, and I am sure elsewhere as well, can not afford to have port and transportation workers denied access or repeated delays in access due to faulty technology. Whatever technology is used to implement TWIC, it must support commercially acceptable error rates, processing times, and overall reliability. While I understand your agency is in the process of reviewing comments on the TWIC technology standards recommend by the NAMSAC, I would like to know what steps your agency is taking to ensure that any technology that is deployed or required to be deployed is error free and economically viable.

Answer. The Transportation Worker Identification Credential will be aligned with the Federal standards for government credentials contained in the National Institute of Standards and Technology's (NIST's) Federal Information Process Standard 201–1 and associated standards such as those in NIST's Special Publication 800–76. 800–76 specifies a false rejection rate (FRR) of less than or equal to 1 percent and a false acceptance rate (FAR) of 1 percent. The FRR is the percentage of incorrectly rejected valid users. The FAR is the percentage of imposters incorrectly matched to a valid user's biometric.

Planning for the pilot programs has been underway since December 2006. A pilot test agreement has been reached with the Port of Long Beach and approval of an agreement with the Port of Los Angeles is expected in the next few months. Discussions are also ongoing with the Port Authority of New York and New Jersey to finalize their participation. TSA, with assistance from other Department of Homeland Security components, is developing a comprehensive Test and Evaluation Master Plan which we anticipate completing this summer. TSA has also been working with the National Institute of Standards and Technology to develop laboratory performance tests to assure baseline performance for this technology, as well as the Space and Naval Warfare Systems Command who will conduct environmental and ruggedness testing.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO HON. EDMUND S. "KIP" HAWLEY

Question. In 2002, the State of Florida enacted a law requiring a Florida Uniform Ports Access Credential (FUPAC) in order to ensure the safety and security of Florida's twelve public seaports. At approximately the same time, Congress passed and the President signed into law the Maritime Transportation Security Act of 2002 (MTSA), which contained many of the same goals.

In an effort to harmonize and maximize the effectiveness of both programs, the State of Florida signed a Memorandum of Understanding (MOU) with the Transportation Security Administration (TSA) in September 2003 to design and implement a prototype Transportation Worker Identification Credential (TWIC) in the State of Florida. The goal of the MOU was to create a prototype credential that could meet both the state and Federal port security requirements. Since that time, Florida has been the only state to reach a level of readiness to actually implement such an access credential, including the ability to read the card electronically for each entry and exit from the state's public seaports.

The TWIC final rule published in the *Federal Register* allows for equivalent credentials, but seems to imply that those equivalencies will only apply to certain Department of Defense (DOD) cards or credentials. As the rule makes clear, there is a need for national, uniform standards for the issuance of a TWIC. However, in light of the pre-existing MOU and pilot TWIC program, has the TSA considered grandfathering the FUPAC as an equivalent credential to the Federal TWIC?

Answer. The Transportation Security Administration (TSA) partnered with the Florida Department of Highway Safety and Motor Vehicles, via a signed Memorandum of Understanding on October 17, 2003, "to mutually plan for and execute the implementation of the Transportation Worker Identification Credential (TWIC) as the common inter-modal credential to support both programs and to fulfill the vision of the TWIC and the requirement of the Florida Uniform Port Access Credential Program (FUPAC) as outlined in Florida statute (311.12 and 311.125)."

The TWIC Final Rule does not preempt any entity from issuing credentials in addition to the TWIC. TSA continues to work closely with Florida officials to align FUPAC with the TWIC program. Both parties agree that it would be in the best interest of port workers to issue a single credential. TSA has informed the State of Florida that it cannot grandfather FUPAC as an equivalent credential or substitute FUPAC for TWIC, because of key distinctions between their requirements and the TWIC. The two parties are discussing options for Florida to integrate the TWIC into their process to comply with their state regulations.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DAVID VITTER TO HON. EDMUND S. "KIP" HAWLEY

Question 1. Given the delays in the process and so many unanswered questions at this late date, what are you doing to ensure that the maritime industry will have time to meet requirements without unacceptable disruptions?

Answer. Each port will receive notice prior to the commencement of enrollment at the port. The Captain of the Port will assess the progress of enrollment levels and will publish, at least 30 days in advance of the effective date, notice to comply with Transportation Worker Identification Credential (TWIC) requirements. This provision was included in the regulations to ensure the vast majority of individuals within a COTP zone requiring a TWIC would have at least 3 months official notice of the compliance date.

Question 2. I feel that the Department did not follow Congressional intent in developing an interim work process. From what I have heard from my constituents in the various maritime industries, without a significant interim period on the front end, it seems that the maritime industries will either have to pay workers to not work while they wait for the TWIC process or lose the employees and face a potential labor shortage.

Answer. A new hire provision is included in the TWIC final rule. This provision is intended to limit the risk presented by an individual who has not undergone a full security threat assessment and is waiting to receive a TWIC while balancing the need to enable individuals to begin work as soon as possible. This provision enables direct employees of the owner or operator, who comply with additional interim requirements, to be eligible for access within 3 days of enrolling for their TWIC for up to 30 days, with an additional 30 days if necessary (upon approval by the Coast Guard), while awaiting TWIC issuance.

Question 3. Can you explain the difference between the thoroughness of an interim security check and a longer term security check?

Answer. The interim security check conducted on port workers last year was a name-based/biographic check of watch lists and databases related to terrorism and legal status. Employers submitted employee names and limited biographic data for the interim check. The interim check did not include the fingerprint-based criminal history records check that will be conducted prior to issuing a credential as part of the Transportation Worker Identification Credential (TWIC) program. The information used to conduct the TWIC security threat assessment will be gathered by TWIC enrollment personnel and will be checked against specific identity documents presented and verified at the time of enrollment. The security threat assessment also includes a fingerprint-based criminal history records check.

The interim check was not intended to replace the TWIC program nor was it intended to capture the entire maritime port worker population. Rather, it was an immediate security measure designed to check those populations employed within the port area and with frequent access, such as employees of facility and vessel operators and longshore labor. A broader maritime port worker population will be covered when the TWIC program is fully implemented.

Question 4. The rule on TWIC allows 1 month for workers to replace a lost card. This seems to create a problem in that mariners often work for 30 day shifts. If a mariner loses a card and files for a replacement, they would almost certainly be onboard a vessel when their work authority runs out. Did you give any consideration to the operations of vessels when you issued this rule? Are you considering any up-

dates to avoid the situation of someone being unable to legally work while on a vessel out to sea?

Answer. Yes, vessel operations were considered during the development of the TWIC regulations. Field guidance pertaining to a mariner's inability to visit an enrollment center while underway, is currently being considered for inclusion into a Navigation and Vessel Inspection Circular (NVIC). The NVIC will serve as robust field guidance to assist the Coast Guard Captain of the Port and the maritime industry with TWIC implementation and compliance and the maritime industry in operationalizing the statutory and regulatory requirements of TWIC implementation and compliance.

Question 5. As we have seen with the No-Fly List, sometimes people with similar names are denied access to a flight. What resources will you have in place to make sure that problems of mistaken identities or other issues such as that are dealt with quickly so that TWIC applicants are not unreasonably delayed?

Answer. During Transportation Worker Identification Credential (TWIC) enrollment, the applicant provides biometrics and extensive biographic information, well beyond what is available in the No-Fly process that will significantly reduce the number of individuals identified as potential matches.

The initial adjudication process includes an assessment of each applicant's criminal history and citizenship status. Each applicant is also vetted against relevant intelligence databases. Any applicant with potential disqualifying information is assessed through a process of review by multiple trained adjudicators who determine whether the applicant meets the requirements to hold a TWIC. The process is designed to reduce the risk of improperly adjudicating the applicant while minimizing the time of adjudication. Legal counsel is available to the adjudicators to help resolve issues before reaching a decision concerning an applicant's threat to transportation security within the confines of the regulation.

TWIC applicants who are initially determined to present a security risk are advised by letter of this initial finding. The letter explains the applicant's right to appeal the finding or request a waiver as appropriate. If the applicant wishes to appeal an initial determination, the applicant has the opportunity to request the records on which the initial determination was based. The applicant may submit additional information, such as corrected official records on his or her criminal history, citizenship status, or other relevant information that may allow the Transportation Security Administration (TSA) to rescind the initial determination. When possible, TSA will make a reasonable attempt to assist the applicant by identifying or acquiring information that enables TSA to grant a favorable final determination. The waiver process is similar, although waivers are based on an assessment of risk despite the applicant being ineligible for a TWIC due to the applicant's criminal history. This information is reviewed by a board of TSA personnel. If a waiver or appeal is denied, the applicant has the right to request review by an Administrative Law Judge who then provides a recommendation on the merits of each individual case.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO RADM BRIAN SALERNO

Question 1. The SAFE Port Act requires the Coast Guard and the TSA to concurrently process applications for individuals applying for a TWIC card and a Merchant Mariner Document (MMD). How are the Coast Guard and the TSA addressing this issue? What steps are you taking to ensure the MMD applications are processed as expeditiously as possible?

Where is the Coast Guard in the process of completing a companion rule to consolidate existing MMDs and to streamline the application process for mariners who are also applying for a TWIC?

What processes and procedures has the Coast Guard established to ensure that information is appropriately shared with the TSA and that mariners do not endure excessive delays in obtaining their MMD?

Answer. The Coast Guard and TSA have agreed to share information, but all the details have not been finalized at this time. We will publish the details before the TWIC requirement come into effect for mariners (September 25, 2008, per the TWIC final rule). In the meantime, in an effort to ensure MMD applications are processed as quickly and consistently as possible and reduce delays in obtaining MMDs, the National Maritime Center (NMC) is in the process of centralizing the mariner evaluation process in Martinsburg, WV. The NMC is also working on a paperless application process.

Public comments for the Consolidated Merchant Mariner Credential (MMC) Notice of Proposed Rulemaking (NPRM) closed on April 25, 2007 and are being reviewed. An MMC format decision meeting is scheduled for May 2007. The MMC final rule will be published and in effect prior to the requirement for mariners to obtain a TWIC.

The USCG and TSA are currently working on resolving a number of issues related to:

- Printing the TWIC digital photo on the MMC in International Civil Aviation Organization (ICAO) format.
- Printing the TWIC digital fingerprints on the MMC in accordance with ILO185–SID convention.
- Ensuring the Coast Guard is able to retrieve TWIC mariner applicant FBI information, for the purpose of additional safety vetting, after the security vetting is complete.
- Passing, from TSA to the Coast Guard, the names of mariners who apply for a TWIC and are denied by TSA.

Question 2. How does the Coast Guard plan to handle the potential increased Administrative Law Judge (ALJ) case load when the TWIC enrollment process begins?

Answer. The Coast Guard believes that there may be a notable increase in ALJ case load once TWIC enrollment begins. However, we do not anticipate that this increase in case load will come at the cost of other important Coast Guard work. The Coast Guard has performed ALJ work for other government agencies, including the Transportation Security Administration (TSA), via reimbursable agreement for some time. Any new resources necessary to support the increase in case load; including Federal employees will be funded via a modification to the current reimbursable agreement with TSA.

Question 3. Did the Coast Guard participate in the negotiations regarding the development the International Civil Aviation Organization (ICAO) Standard? Why has the United States declined to ratify the resolution? Do you think this poses additional burdens for U.S.-flag vessels operating in international commerce?

Answer. No, the Coast Guard did not participate in development of the ICAO standard. However, the Coast Guard did participate in the development of the ILO Convention 185, which specifies an ICAO standard for the printing of information on a Seafarer's Identity Document.

The Coast Guard defers to the State Department regarding why the U.S. decided not to ratify this convention. The Coast Guard has not evaluated the effect that the ICAO Standard would have on U.S.-flag vessels. However, regardless of ratification, the Coast Guard intends on developing the Merchant Mariner's Credential in a manner that is compliant with ILO Convention 185 to ensure that U.S. mariners comply with this convention should it be mandatory in a foreign port-of-call.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARIA CANTWELL TO RADM BRIAN SALERNO

Question. Rear Admiral Salerno, I have heard back from several ports in my state that the Coast Guard has done a good job in keeping port managers informed on issues relating to TWIC regulation and implementation. As you know, Washington State falls within District 13 and is served by both Sector Seattle and Sector Portland. Are you aware of any inconsistencies between Sectors within District 13 regarding TWIC implementation policies? For example, there are a number of non-traditional port facilities in my state where there may be a need for greater flexibility in TWIC implementation. How do you ensure consistency between Sectors so there is not confusion on TWIC policy between non-traditional ports in the same state?

Answer. The Coast Guard is not aware of any inconsistencies between Sectors within District 13 regarding TWIC implementation policies. Flexibility in determining compliance dates does exist however in that compliance dates will be established based on input from the Captain of the Port (COTP), Transportation Security Administration (TSA) and TSA's contractor Lockheed Martin. It is the CG's and TSA's goal to ensure the majority of workers within a COTP Zone have ample opportunity to apply for and receive a TWIC during the initial enrollment periods before setting a compliance date. The USCG is currently developing robust field guidance in the form of a Navigation and Vessel Inspection Circular (NVIC) to assist COTP and the maritime industry in operationalizing the statutory and regulatory requirements of TWIC implementation and compliance. National consistency is one

of the USCG's goals regarding the TWIC program and the NVIC is a useful tool to assist in that endeavor.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO RADM BRIAN SALERNO

Question 1. Primary law enforcement responsibility in US ports rests with a port authority police force or a local law enforcement organization and USCG personnel are generally not onsite everyday. How does the USCG plan to accommodate this provision and minimize the impact to local law enforcement by needing to hold an individual "until Coast Guard personnel arrives to confiscate the TWIC card?" Wouldn't it make more sense to allow a bona fide law enforcement official to confiscate a TWIC card based on reasonable cause?

Answer. The Coast Guard is currently exploring the legal and operational issues involved in allowing bona fide law enforcement officials to confiscate TWICs based on reasonable cause. This is one of several options currently being evaluated as the Coast Guard develops the policy and field guidance associated with TWIC enforcement. The USCG is currently developing robust field guidance in the form of a Navigation and Vessel Inspection Circular (NVIC) to assist COTP and the maritime industry in operationalizing the statutory and regulatory requirements of TWIC implementation and compliance.

Question 2. In a joint TSA/USCG Notice of Proposed Rulemaking that was published in May 2006, a contact reader with PIN technology was proposed. Industry vehemently opposed this technology solution because of the negative impact it would have on terminal efficiency. Where does the USCG now stand on the issue?

Answer. The proposed requirements for biometric readers and Personal Identification Number (PIN) usage by Transportation Worker Identification Credential (TWIC) holders prior to accessing secure areas of regulated facilities and vessels were excluded from the Final Rule which was published on January 25, 2007. Under the existing rule, the TWIC is required to be utilized as a visual identity badge, but a PIN will not be required for routine unescorted access to facilities or vessels. A PIN however will be necessary to "unlock" the biometric template stored in the TWIC integrated circuit chip, to facilitate the holder's authentication during USCG spot checks. Spot checks are not anticipated to have a negative impact on terminal efficiency.

The TSA and the USCG are currently evaluating options, including the presence or absence of a PIN requirement, for a contactless biometric specification for TWICs and readers with this capability. During this process, we are taking serious consideration of comments received from regulated industry and labor, including comments from the National Maritime Security Advisory Committee, on the requirement for a PIN, but no decision has been reached yet. The specification will be published and tested in operational environments, pursuant to the SAFE Port Act. Implementation will require a follow-on rulemaking effort.

Question 3. The National Maritime Security Advisory Committee (NMSAC) has recommended that the transmission of the biometric fingerprint template from the TWIC card to the card reader not be encrypted because it would complicate the processing, add unnecessary cost and maintenance concerns as well as slow down terminal operations. On the other hand, the biometric industry has recommended encryption even though they admit that a fingerprint template cannot be re-engineered into an identifiable fingerprint and offers no privacy protection. Where is the USCG on the issue of encryption? What is the timeline for making a final decision on the selected TWIC chip/reader technology? When will it be published? Finally, what is the expected timeline for the publication of the TWIC Phase II NPRM?

Answer. The fingerprint template is considered Personally Identifiable Information (PII) and therefore should be protected. When the template is transmitted from the TWIC to a contactless reader it is subject to being intercepted. Additionally, it is possible to use radio frequency waves to simulate a reader and thus "skim" an unprotected template from a card. Therefore, in allowing contactless operation, the TWIC fingerprint template must be protected in some manner. As NMSAC ruled out using a Personal Identification Number (PIN) to protect the template during transmission, encryption to establish a secure link over which to transmit the template is one way to accomplish this protection.

NMSAC does not believe the protection above which is afforded by the Minutiae template is necessary and therefore their recommendation was to not encrypt the transmission. They did provide an additional specification for encryption with the understanding that encryption might be a government requirement.

Currently if a template were compromised it is unlikely there would be any security or privacy implications. However, as technology moves forward and biometrics become more commonly used, we cannot be certain this will be the case in the future. Therefore, since a person cannot change their fingerprint template if it is compromised, the government must ensure that a level of protection is provided.

The final contactless specification will be published in the *Federal Register* in the coming months. The USCG and the Transportation Security Administration (TSA) have begun work on the TWIC II NPRM and expect to publish it in early 2008.

Question 4. Is encryption contemplated for the TWIC program consistent with the requirements put forth by the DHS in the REAL ID Driver's License program NPRM? Or any other DHS identification card programs now underway?

Answer. Yes. When a biometric template or other PII is being transmitted in a contactless manner or otherwise embedded in an identity document, this information is protected. The best example is HSPD–12/FIPS 201 documents, upon which the TWIC standard was based. REAL ID does not require the collection of biometrics. However, DHS proposed that PII embedded in the mag stripe be encrypted.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO NORMAN J. RABKIN

Question 1. You state in your testimony that TSA has developed a schedule for enrolling workers and issuing TWIC cards at ports. Have you seen this deployment schedule, and is it based on risk? Did you find it to be reasonable and achievable schedule?

Answer. TSA reported to us that the agency has developed a schedule for enrolling workers and issuing TWIC cards at ports, but we have not seen a copy of this schedule. As a result, we did not evaluate whether the schedule is based on risk or is reasonable.

Question 2. When you reviewed the prototype contract in your September 2006 report, did you find how many card readers were deployed, and actually tested? If so, at which locations were they tested?

Answer. According to the TWIC prototype report, 99 TWIC card readers were installed at 19 locations during prototype testing. According to the prototype report, these locations included: MacArthur Airport in New York; Los Angeles International Airport; Broadway Terminal in New Jersey; the Maritime Exchange of the Delaware River and Bay; Gloucester Terminal in New Jersey; the Amtrak Operations Center in Delaware; the Ports of Los Angeles and Long Beach; Wilmington, Delaware; Pensacola, Panama City, Fernandina, Canaveral, and Manatee, Florida; and 5 private port terminal facilities at the Ports of Los Angeles and Long Beach.

Question 3. As the Coast Guard moves forward with completing a companion rule to consolidate existing mariner credentials, I believe it is important for the Committee to have a better understanding of the impacts these cumulative fees are having on the industry. Can you please provide a summary of the procedures and the costs a mariner incurs to serve on a U.S.-flag vessel?

Answer. According to the Coast Guard, to qualify for issuance of an entry-level merchant marine license or entry-level rating endorsed on a Merchant Mariner Document (MMD), an applicant must acquire required sea service experience, complete training specified in regulation, and pass a drug screen and physical examination. This information is submitted to a Coast Guard Regional Examination Center for evaluation. The applicant must also appear once during the evaluation process to be identified and be fingerprinted. If the evaluation shows that the applicant meets all of the requirements for the credential and a background check and review of the National Driver Register are satisfactory, the applicant must then demonstrate professional competence by passing an examination or completing training that substitutes for the examination. No examination is required for entry-level ratings.

According to the Coast Guard, the cost that a merchant mariner incurs to serve on a U.S. flag vessel can vary based on region of the country and other factors. Coast Guard officials provided an estimate of these costs as follows:

Cost category	Entry level officer		Entry level rating	
	Seagoing	Inland	Seagoing	Inland
Training	$30,000	$2,000	$1,000	$0
Physical	75	75	50	50
Drug Screening	85	85	80	80
User Fees	300	300	140	140

Cost category	Entry level officer		Entry level rating	
	Seagoing	Inland	Seagoing	Inland
Travel/Miscellaneous	1,000	800	250	250
Total Cost	$31,460	$3,260	$1,520	$520

According to the Coast Guard, travel and miscellaneous costs represent the costs of appearing for examination, identification, and fingerprinting. Distance from an examination center will affect travel costs. Travel costs to attend training are included in the cost of training. For the officer levels, the costs are those applicable to an applicant for a license as third mate unlimited (seagoing vessels) or for a license as mate 1,600 gross register tons (inland vessels). These license levels represent common entry points into a seagoing career. In some cases, employers will reimburse applicants for some or all of the costs to qualify for a license or MMD.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TED STEVENS TO NORMAN J. RABKIN

Question 1. Mr. Rabkin, in your written testimony you mentioned both progress made and challenges remaining for the TWIC program. Does TSA have sufficient force and assets to handle this type of large scale program implementation?

Answer. Until TWIC program implementation begins later this year, it is difficult to evaluate whether TSA and the enrollment contractor have dedicated the staff and resources necessary to successfully implement the program. Since we issued our September 2006 report, TSA has added staff to the TWIC program office to better manage the program and established an office to more closely monitor the performance of the enrollment contractor. However, we did not evaluate the number of staff or resources that the TWIC enrollment contractor has dedicated to implementing the program as part of our review. While additional staff with expertise in program and contract management should help TSA to implement the program, it remains to be seen whether TSA and the enrollment contractor will be able to implement the TWIC program on such a large scale covering 770,000 workers at about 3,500 maritime facilities and 5,300 vessels in the required time frames.

Question 2. If not, what suggestions does GAO have to ensure an effective implementation of TWIC?

Answer. Addressing the primary challenges facing the TWIC program is the most important step to ensure effective implementation. TSA and maritime industry stakeholders face several challenges to ensuring that the TWIC program can be implemented successfully. Although TSA has learned from TWIC testing experiences and has taken steps to help address problems that we previously identified, transitioning from limited testing to full scale implementation will be a major challenge. In addition, TSA and its enrollment contractor will also need to educate workers on the new TWIC requirements through an effective communication and coordination strategy, ensure that enrollments begin in a timely manner, and process numerous background checks, appeals, and waivers. Furthermore, TSA and industry stakeholders will also need to ensure that TWIC access control technologies will work effectively in the maritime environment, be compatible with TWIC cards that will be issued, and balance security with the flow of maritime commerce. As TSA works to implement the TWIC program later this year, it will be important that the agency establish clear and reasonable time frames and ensure that all aspects of the TWIC program, including the TWIC access control technologies, are fully tested in the maritime environment.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO NORMAN J. RABKIN

Question 1. While I appreciate TSA's willingness to further study the requirement directing each towing vessel to carry a card reader, I remain concerned about the effect of this requirement on the maritime industry, particularly its small businesses. As you know, there is significant opposition to requiring card readers on every towing vessel. Given that crew sizes on tug boats reportedly run between four and ten mariners, and each of those mariners is well known to other mariners on the tug, as well as management, therefore making any intruder obvious, do you believe a workable compromise could be reached, such as only requiring card readers on vessels employing ten or more mariners?

Answer. According to TSA, the agency will address all requirements regarding TWIC access control technologies, such as biometric card readers, in a second proposed rule that the agency plans to issue during 2008. Until access control requirements are set forth in this proposed rule, it is not clear in what circumstances TWIC card readers will be required on vessels. In addition, the Security and Accountability for Every Port Act of 2006 states that TSA cannot require card readers on vessels unless TSA determines that the vessel is at severe risk or that readers are necessary due to the number of individuals on board. As such, TSA must consider this requirement as well as any public comments regarding the installation on card readers on vessels as part of the second rulemaking in the future.

Question 2. The TWIC application process remains burdensome on workers and the industries depending on them. Easier access to TWIC cards once granted may help relieve some of this burden without causing undue security concerns. Many are concerned about the cumbersome process to apply for a TWIC card, including the long distances some workers will be required to travel to obtain a TWIC card. This is especially true for those in the long haul trucking industry who may end up applying for their card at one enrollment center, but due to the nature of their employment may be far from that center by the time the card is ready. In your opinion, would allowing applicants to designate that cards be returned to a different enrollment center than where they originally applied or alternatively including a mechanism to mail cards to an applicant's home or office be realistic fixes for this problem? If not, what do you propose as an alternative?

Answer. According to TSA, shipping a TWIC card to an enrollment center, other than the one at which enrollment took place, was considered as well as mailing cards directly to the applicant during the planning stages of the program. TSA officials determined that it would be preferable to follow the process set forth in Federal Information Processing Standard 1, which calls for individuals to retrieve identification credentials in person so that their identity can be verified. According to TSA, mailing TWIC cards directly to the individual raises security concerns because TSA would not be able to ensure the individual receiving the card was in fact the individual that applied for the card. However, TSA officials stated that they understand that the return visit to the enrollment center will be inconvenient for some TWIC applicants and may reconsider this process in the future to reduce burden on the affected population. Our review focused on the results of the TWIC prototype test and did not evaluate the feasibility of having TWIC cards mailed to a worker's home or office or any other alternative method of picking up a TWIC card.

Question 3. The costs associated with TWIC may be a barrier for some workers and businesses. While I understand those costs may compare favorably with other card fees, they remain a burden for the temporary, seasonal labor in the maritime industry. Of particular concern is the fact that an applicant must pay for the full price of the application up front, leaving those applicants who are denied cards paying for the production of cards they do not receive. One potential solution may be not to reduce the overall costs, but the schedule on which they are paid. In your opinion, would it be possible for TSA to charge only for the cost of processing the application and the security assessment up front, with the balance to be paid should a card be granted?

Answer. According to TSA officials, the agency considered allowing workers to initially pay for the enrollment and threat assessment portion of the TWIC fee and pay the remaining balance when the card is issued. However, TSA officials stated that the current process of payment and fee collection provides the best value to the total population and limits the overall cost of the TWIC card. According to TSA, while workers ultimately denied a TWIC may pay for the card production and issuance portion of program costs, they benefit from having all applicants sharing equally in the cost of the process. Workers whose criminal history would otherwise result in denial of a TWIC may request a waiver through the TSA redress process and review by an administrative law judge. Adopting a position that TWIC applicants should only pay for the services they directly receive could result in considerable costs to those applicants utilizing this redress process. As part of our review, we did not evaluate TSA's rationale for requiring the fee to be paid in full at the time of enrollment or the feasibility of any alternate methods of paying for the TWIC card.

Question 4. The goal of the TWIC program is to strengthen the security of our transportation system, starting with the implementation of a pilot without unintended consequences. Unfortunately, a host of issues have plagued the successful implementation of the pilot, including an incomplete management plan to date, lack of contract accountability, and ever-increasing costs to implement the program. I am concerned that if we don't fix these problems soon, we jeopardize the health of our

workforce, strength of our economy, and overall, security of our Nation. Given these are just some of the implementation issues since the TWIC pilot was first authorized in 2001, please describe how our workforce and economy has been indirectly impacted by these delays.

Answer. Our past work on the TWIC program has identified program delays, problems regarding testing and contract management, and additional challenges that the program faces. However, we did not evaluate either the direct or indirect impact that TWIC program delays and problems have had on the workforce and economy.

Question 5. It is my understanding that the TWIC system will not be interoperable with international standards. I am concerned that without uniformity of international standards, non-U.S. crewman will be exempt from complying with our security provisions when entering U.S. ports. Do you think it is necessary to establish an uniform international ID standard? What is the agency's plan to sync the TWIC system with the current biometric technology used by the United Nations and developed by the International Civil Aviation Organization (ICAO)?

Answer. According to TSA, the agency determined that it is preferable to have TWIC be interoperable with credentials issued to U.S. Federal standards rather than ICAO standards for international travel documents. TSA officials stated that TWIC is not intended for international travel, but does have potential applications with other U.S. Government credentials. Therefore, to achieve maximum interoperability with other programs, security and protection of personal information, TWIC follows the Federal Government standards for biometric credentials which are contained in FIPS 201 and the American National Standards Institute (ANSI) publication 378. TSA plans to continue monitoring international developments and protocols to determine what if any benefits to the program they provide. As part of our review, we did not evaluate the interoperability of the TWIC system with international standards or TSA's plans to synchronize the TWIC system with biometric technologies used by the United Nations or ICAO. In addition, we did not examine the need to establish a uniform international identification standard.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DANIEL K. INOUYE TO LISA B. HIMBER

Question. How would you advise the TSA and the Coast Guard to address the seasonal labor issue for the maritime industry?

Answer. After discussion with various facility operators and labor organizations, the issue remains one for which there is no clear answer. While many members are in favor of a provision that allows for a "temporary credential" which would be capped after an appropriate number of port visits (*e.g.,* after the third time, the worker would be required to obtain a TWIC for access), others see this as difficult to monitor.

We respectfully request that this issue be tabled until after the Coast Guard finalizes its Navigation and Vessel Inspection Circular document, which will provide guidance on the escort provisions. In addition, we expect it will be necessary to reevaluate this issue once the TWIC program is underway and the impact can be accurately assessed.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. FRANK R. LAUTENBERG TO LISA B. HIMBER

Question. I understand you have been involved in efforts to develop biometric standards for the TWIC card readers that are "contact-less"—meaning they would not require entering a password, for example. Doesn't this type of technology reflect the "lowest common denominator" as opposed to the highest possible level of security?

Answer. The term "contactless" refers to the fact that a card can be read without the need to insert or swipe it into a reader. The maritime industry believes it is important to use contactless TWIC readers because contact readers are more quickly subject to damage by the normal usage, the environment, and vandalism.

A contactless biometric may or may not require the use of a Personal Identification Number (PIN) or other password. The National Maritime Security Advisory Committee recommended to DHS that under normal operating conditions (*i.e.,* MARSEC I) those who seek access to regulated facilities and vessels be required to present their TWICs only. During times of heightened security (MARSEC II and

III), individuals would be required to present a biometric for verification in addition to the card.

However, it is important note that during normal operations, persons seeking access to a regulated area must verify that they have a legitimate need to enter, and in most cases, the individual's name must be on a gate or appointment list.

In keeping with the overarching philosophy that DHS must seek to find an appropriate balance between enhanced security and facilitation of commerce, the maritime industry believes that adding a requirement for use of a PIN presents an additional and largely unnecessary potential point of failure which could lead to lengthy delays in vessel and cargo processing.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO CAPT. PAUL KAIPO POMAIKAI, SR.

Question 1. The interim work authority process the TSA provided for in the final rule appears to be more restrictive than what your industry was hoping for. As I understand it, newly hired workers must apply for their TWIC, pay the fee, pass the named-based background check from TSA and still be accompanied by an individual with a TWIC card at all times while in a port. Is my understanding of this process correct? Can you explain how that presents difficulties to your operations?

Answer. Yes, that is the process that is outlined in the final rule. The biggest problem with the interim work authority process provided by TSA is that the process doesn't begin until a new hire has traveled to a TWIC enrollment center and applied for his or her TWIC in person, plus paid the $137 fee. This is a problem, first of all, because of the burden it imposes on mariners. When you're a young person seeking a job who doesn't even know yet if the maritime industry is right for you, it's a big hurdle to be told you've got to fly to another island or take a bus halfway across the state to a TWIC enrollment center. And, $137 is no small change when you haven't even started working yet. From an employer perspective, companies in our industry are very concerned that folks considering employment in our industry will look at these burdens and say, "No thanks. I think I'll go do something else." The maritime industry is already facing a severe personnel shortage, and the last thing we want to do is set up barriers to entry that discourage prospective employees from coming to work for us.

The second problem with the TSA process is the additional time it requires before a new hire can be put to work on a vessel. As a practical matter, an employer will not want to send a new hire to a TWIC enrollment center to start the process until the new hire has passed a drug screen, taken a physical, and had his or her references checked. What all of that means is that it may be a week before the individual goes to the TWIC enrollment center and "starts the clock" on the interim work authority process.

We could address both of these issues—reducing burdens on mariners that discourage new entrants into the industry, *and* enabling employers to put new employees to work more quickly—if we could begin the process with a computerized check against the terrorist watch list instead of a trip to the TWIC enrollment center. This approach would not diminish security in any way, since it's the same check that TSA is proposing to use to grant interim work authority in the final rule. But, it would save a mariner the time and expense of a trip to the enrollment center, and it could be done immediately, concurrently with the drug screen, physical, and reference checks that the company will conduct. This would enable mariners to get to work sooner, since the terrorist watch list check could be in process while the mariner is completing these other essential steps in the new hire process.

After a reasonable period of time—say, 90 days—a new hire that intended to stay in the industry would be required to go the enrollment center, apply for a TWIC, and pay the $137 fee. This would be a meaningful interim work authority provision that would work for the maritime industry without compromising security.

Question 2. As the Coast Guard moves forward with completing a companion rule to consolidate existing mariner credentials, I believe it is important for the Committee to have a better understanding of the impacts these cumulative fees are having on the industry. Can you please provide the Committee a summary of procedures and of the costs a mariner incurs to serve on U.S.-flag vessels?

Answer. A career in the maritime industry is rewarding, but it's also expensive. In addition to the cost of the TWIC—$137 for a five-year credential—mariners who are required to hold Coast Guard licenses or Merchant Mariner's Documents also pay user fees for those credentials. Those fees range from $140 for an original MMD with no endorsement, to $255 for a license as Mate or Master of Towing Vessels, to $280 for an MMD with a tankerman endorsement. As with the TWIC, though,

the cost of the credential itself is only part of the story—it's the hidden costs like the time and expense of travel to a TWIC enrollment center or Coast Guard Regional Exam Center that are even more significant for most mariners. An even more serious concern of many mariners today is the cost of medical tests that may be necessary to prove that a mariner is medically qualified for a license or document. A draft Coast Guard policy document (a Navigation and Vessel Inspection Circular, or NVIC, on medical and physical standards for merchant mariner credentials) would require a mariner who has one of more than 200 listed medical conditions to provide extensive information to the Coast Guard. In some cases, the required information includes consultations with specialists and medical test results that may or may not be covered by insurance.

For mariners in the coastal and oceangoing towing industry, there are also enormous expenses associated with the training courses required for an STCW certificate. (STCW is the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers.).

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARIA CANTWELL TO CAPT. PAUL KAIPO POMAIKAI, SR.

Question. You have stated your concern regarding the proposal to require card readers on every towing vessel. In your opinion, would requiring card readers only on vessels employing larger numbers of mariners (for example, ten or more) be a workable middle ground? Would such a compromise help alleviate the burden this requirement could cause on those in the maritime industry?

Answer. This would certainly provide an acceptable compromise. The SAFE Port Act gives DHS the authority to limit the card reader requirement to vessels with more than a certain number of crew, to be determined by the agency. We suggest that, at a minimum, vessels with 12 or fewer crew members requiring a TWIC should *not* be required to have a card reader installed on board. Card readers are simply unnecessary for vessels with small crews, such as towing vessels whose crew sizes typically range from four to ten mariners. In an average U.S.-flagged towing vessel operation, every employee is known to management and fellow crewmembers. A stranger onboard the vessel is immediately obvious. Personal knowledge of fellow employees provides a higher security standard than reliance upon an electronic reader, no matter how sophisticated the technology employed. Access control procedures are already included as part of a Coast Guard-approved vessel security plan.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DANIEL K. INOUYE TO MICHAEL J. RODRIGUEZ

Question. Why is it important that we utilize the International Civil Aviation Organization standards for U.S.-flag vessels operating in international commerce?

Answer. There are several important reasons for using the International Civil Aviation Organization standards to implement the Transportation Worker Identification Credential.

First, we agree wholeheartedly that the implementation of a uniform Transportation Worker Identification Credential (TWIC) system is an important tool in the effort to prevent maritime terrorism. Maritime workers, whether they are longshoremen, seafarers or harbor pilots are on the front lines. We are deeply disappointed by TSA's inability to establish a program to identify and bar from security-sensitive transportation jobs those individuals who clearly pose a security risk. We shared the Committee's frustration when we learned, during the April 12, 2007 hearing, that the schedule for TWIC implementation is falling so far behind. We believe that one of the reasons it is falling behind lies with the policy decision to use the unproven and inappropriate FIPS–201 standard for the biometric identity cards in the TWIC program, rather than the widely used and internationally recognized International Civil Aviation Organization (ICAO) standards.

ICAO is an organization within the United Nations with headquarters in Montreal. It was established by international convention in Chicago in 1946. Today ICAO has 190 member states including the United States. Our country is also a member of ICAO's governing council.

Civil aviation is a critical service that is vital to the global economy. Therefore, ICAO members work toward standards of practice in biometric identity systems for machine readable travel documents to facilitate the movement by air of persons around the world. Maritime shipping is likewise essential to our global society. The movement of cargo, passengers and workers through our ports would also benefit from the implementation of uniform international standards.

We believe Congress anticipated the need for compatibility between identity documents for transportation workers in the Maritime Transportation Security Act of 2002 (MTSA) section 103(a). The MTSA encourages the U.S. Coast Guard to:

> ". . . negotiate an international agreement, or an amendment to an international agreement, that provides for a uniform, comprehensive, international system of identification for seafarers that will enable the United States and another country to establish authoritatively the identity of any seafarer aboard a vessel within the jurisdiction, including the territorial waters, of the United States or such other country."

Likewise, Section 303(b)(1) of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act) very clearly establishes Congress's intent that the US system of machine readable, tamper-resistant travel documents conform to international standards. The section reads, in part:

> "The Attorney General and the Secretary of State shall jointly establish document authentication standards and biometric identifier standards to be employed on such visas and other travel and entry documents from among those biometric identifiers recognized by domestic and international standards organizations."

Furthermore, in section 110(a) of the SAFE Port Act of 2006 (SAFE Port Act), Congress expressed its desire for the Secretary of Homeland Security to expedite the crewmember identification process when it amended the MTSA. The amended section 70111(a) of the MTSA now reads:

> "*Requirement.*—Not later than one year after the date of enactment of the SAFE Port Act, the Secretary, in consultation with the Attorney General and the Secretary of State, shall require crewmembers on vessels calling at United States ports to carry and present on demand any identification that the Secretary decides is necessary."

If foreign crewmembers will be carrying ICAO-compliant identity documents, it is difficult to imagine why the Department of Homeland Security has selected a transportation worker identification system that is not compatible with ICAO. We feel that if the TWIC program were designed to comply with the ICAO standards, then TSA and the U.S. Coast Guard would have a much greater chance of meeting the deadlines established by Congress.

Given the unambiguous intent of Congress as expressed in the MTSA and the Border Security Act that the TWIC and U.S. travel documents conform to international standards, its is clear that Congress recognized the value of globally interoperable systems and has directed the relevant agencies to pursue interoperability. What is not clear is why TSA and the Coast Guard have ignored this aspect of the Congressional mandate and have chosen instead an internal Federal Government standard for the TWIC that will never be interoperable with international standards and was untested and unproven on the massive scale required for the TWIC program.

The International Labor Organization (ILO), the United Nations organization responsible for seafarer identity documents, after special sessions, adopted the ILO Seafarer Identity Document (SID) Convention 185 (C–185) in June 2003. The purpose of the SID Convention is to establish uniform interoperable biometric identity document standards to be used in conjunction with the International Maritime Organization's (IMO) International Ship and Port Security Code (ISPS Code) that establishes the international maritime security system. The ISPS Code is the product of an initiative launched by the United States under the auspices of the United Nations organization responsible for the regulation of international shipping, to establish a uniform international maritime transportation security regime. The U.S. Coast Guard's Federal maritime security regulations (33 CFR 104 and 105) are based upon the ISPS Code. In addition to setting out the fundamentals for a comprehensive Seafarer's Identity Document management system, C–185 prescribes the use of the ICAO biometric identifier standards as the basis for the SID. The ICAO standards are currently in use worldwide for passports, visas and other travel documents and cards.

The ICAO standards are a proven and internationally accepted technology for identity documents. The readers and other supporting hardware have also been proven at airports around the world. We believe TWIC should start with this established system and build upon it as technology advances and new capabilities emerge.

There are several benefits to this approach for the TWIC program.

First, the Department of Homeland Security and the American taxpayer will not have to invent a new technology. In our view, this is what Congress envisioned in authorizing the TWIC program.

Second, because the SID's carried by seafarers from other nations will be ICAO compliant, port facility operators and the Coast Guard would be able to scan and track the identity documents of foreign seafarers as they enter and exit the United States. Additionally, there would be less of a tendency for facility operators to lock down seafarers aboard their vessels. Lock downs are frequent today, in part, because the seafarers do not have acceptable identity documents. The identity card carried by a professional mariner should allow the mariner the same freedom of movement in the United States that passports and visas give other travelers.

Third, American seafarers would be able to use their TWIC cards abroad for access to facilities in foreign ports. This would have the effect of ensuring American seafarers will have free access for shore leave, crew changes, and travel to and from their ships.

By starting from a straightforward and uncomplicated foundation—by adopting the same proven technology that is widely used for access control of foreign visitors to the United States as well as at international airports and in foreign ports, we can dramatically reduce the problems with the present TWIC program and increase the ease and speed of implementation of the TWIC.

We understand that TSA and the Coast Guard have invested a great deal of time and money in trying to develop a new technology for the TWIC program. However, TSA has issued not even a single working TWIC card 5 years after being directed to do so by Congress. We believe it is not too late to get the program right by moving forward with a simple, internationally accepted and interoperable identification program based on the ICAO standards.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO MICHAEL J. RODRIGUEZ

Question 1. How many states are moving forward with their own security credentialing programs in the absence of a Federal system?

Answer. At this point, we are aware of only one state—Florida—in which individual ports have each put in place their own unique security credentialing and access control programs. However, it is important to understand that under the existing statute, there is no Federal preemption over such programs—not only each state, but each individual port and individual facilities within the same port are free to impose their own requirements for access control and security credentialing. This means that mariners who have a Federal TWIC card and who work aboard vessels that trade from port to port, from state to state, and from the United States to overseas ports will nevertheless be subjected to numerous costly and time-consuming background checks and application processes, delaying and impeding their opportunity to do their jobs and earn their livelihood and unnecessarily disrupting the movement of American commerce.

In addition, the lack of a Federal program could mean that mariners: (1) who do not possess a credential issued by the local facility will be prohibited from taking shore leave or joining a vessel while the vessel is docked at the facility, (2) will have to pay each facility for an access card, (3) will have to continue to pay outrageous fees for escort and security services or face imprisonment aboard their vessels, and (4) will be discouraged from remaining in the industry by additional, unnecessary administrative and financial burdens.

The preamble to TSA's Final Rule on TWIC (January 25, 2007) on the question of Federal preemption states:

> "Under this rulemaking, States will not be preempted from instituting their own background checks or badging systems in addition to the TWIC."

In the recently published USCG circular that contains guidance for the implementation of the TWIC program port facilities are advised that they may incorporate the TWIC into their own unique existing access control systems.

It is clear that if individual states and port facilities are permitted to retain their own unique access control systems, the national character of the TWIC card will be destroyed and the TWIC program will be worthless from the standpoint of mariners, ship service personnel, long haul truck drivers, rail crews and other traveling workers who require a single credential that can be used across the entire system.

Transportation workers require a universally accepted card that can be used across all ports where their employment may take them. Such workers are an integral part of the transportation system that makes interstate and foreign commerce

possible. Imposing additional local requirements that demand numerous applications, background checks and fees, perhaps for dozens of individual cards, clearly places an unreasonable burden on interstate and foreign commerce. There is an urgent need for Federal laws and regulations governing the TWIC to preempt any state or local requirements on the same subject matter for such workers.

We believe that unless the Federal Government acts to ensure that the Federal TWIC preempts any and all state and local programs, the maritime workforce will be negatively affected and the efficient flow of commerce will be impeded without the achievement of any additional security benefits for our Nation. Requiring maritime workers to obtain a separate access control credential for every port, facility and terminal at which their vessel calls or at which they work will subject American maritime transportation workers to additional financial and administrative burdens, discouraging Americans from entering our industry and encouraging others to leave the industry for other employment—adversely affecting the civilian maritime manpower base relied upon by the Department of Defense.

From a security standpoint, there is nothing to be gained from subjecting American mariners to the whims and vagaries of each individual state, port and facility that decides to issue its own access and security credential. The final rule to implement the Federal TWIC program has been published and these national requirements, and not local requirements, should prevail.

Question 2. How long do you think they will wait for the DHS to get this right?

Answer. Although we do not have access to information regarding the intentions of individual states, ports and facilities, we believe it is fair to conclude that the legitimate concerns about the risks of a maritime-related terrorist act and the delays in implementing a Federal program will lead to more state and local access control systems. We understand these concerns, and we understand why states, ports and individual facilities may see the need to act unilaterally to fill a vacuum. We also understand that the more this happens, the more disruptive it will be for maritime commerce.

To the degree to which states, ports and facilities act, each different system will require a separate application process, a separate background check, separate administrative procedures, and separate paperwork burdens. This will not enhance security as much as cause confusion and disruptions. We reiterate that the best way for the Federal Government to act quickly and efficiently, and to fulfill its responsibilities to protect national security and to encourage the unimpeded flow of commerce, is to adopt the ICAO standards we referenced previously and to ensure that the Federal system preempts all others. Acting expeditiously and forcefully is, in our opinion, the best way for the Federal Government to "get it right".

We thank the Committee for the opportunity to give testimony on the TWIC program and we are pleased to answer these questions. We look forward to continuing to assist the Committee in whatever manner necessary, including bringing in technical experts who can speak with greater authority on the technical aspects of our views.

○