



JOINT WRITTEN STATEMENT OF

**KELLI ANN WALTHER, ACTING DEPUTY ASSISTANT SECRETARY, SCREENING
COORDINATION OFFICE, OFFICE OF POLICY**

**REAR ADMIRAL JOSEPH SERVIDIO, ASSISTANT COMMANDANT FOR PREVENTION
POLICY, U.S. COAST GUARD**

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

HOUSE COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

JUNE 28, 2012

The Department of Homeland Security (DHS) appreciates the opportunity to appear before the Committee to highlight our work on the Transportation Worker Identification Credential (TWIC) Program, including how it fits into the larger DHS maritime security strategy, its progress to-date in enhancing security, and plans for the future.

DHS understands that there is no one-size-fits-all maritime security solution. The maritime environment is a complicated one, and like our land and air borders, a layered approach offers the best defense. In the maritime domain, these layers look at our U.S. ports and waterways, coastal zone, the open ocean, as well as foreign ports. To fulfill a security mission of such scale, DHS leveraged the expertise of its components to develop an awareness of the different potential targets that comprise the maritime domain and to design security measures to counter potential threats.

For example, the U.S. Coast Guard uses Port Security Assessments and requires Facility and Vessel Security Plans to identify and mitigate vulnerabilities of maritime assets. In addition, the Coast Guard requires 96-hour advance notice of arrival for foreign flag vessels and all commercial vessels (foreign or domestic) entering a U.S. port, to have a better understanding of what and whom to expect and when they will arrive.

Coordination across DHS and intelligence organizations, domestic port security assessments, and critical infrastructure protection plans are all layers to protect U.S. ports and waterways. Along the coastal zone, Coast Guard has stations and response boats, and the National Vessel Movement Center and Deepwater Program. In the open ocean, the U.S. conducts long range vessel tracking and the Coast Guard continues joint efforts with NORTHCOM. Overseas we continue our Container Security Initiative and C-TPAT.

In pursuit of security solutions, the Department has developed strong partnerships with the private sector, as these partnerships are critical to maritime security measures and to protecting our ports. In most cases, the Federal Government does not own or operate the many assets that comprise the maritime domain, including critical infrastructure and key resources. Therefore, we work closely with our partners to meet homeland security objectives in a manner consistent with their operational needs.

The role of TWIC

The TWIC program, authorized by the Maritime Transportation Security Act of 2002 (MTSA) and the SAFE Port Act, strengthens the security of our nation's ports while facilitating trade through the provision of a tamper-resistant biometric credential to all port workers requiring unescorted access to secure areas of MTSA-regulated port facilities and vessels. The mission of

the TWIC program is to provide a means of positively verifying the identity of those seeking access to secure areas and to conduct security threat assessments, enabling maritime vessel and facility operators to make informed access control decisions. TWIC is a minimum requirement prior to a port facility or vessel regulated by MTSA making an access decision. The Federal government is not making those access decisions, and in that respect, this program offers a good example of a strategic security partnership among the Coast Guard, the Transportation Security Administration (TSA), and the private sector. TWIC is one layer, within the array of maritime security measures mentioned above, that enhances port facility and vessel security.

The TWIC Program provides a tamper-resistant biometric credential to eligible maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. No. 107-295). TSA and the Coast Guard jointly administer the TWIC Program. TSA is responsible for enrollment, security threat assessments, and systems operations and maintenance related to TWICs, and the Coast Guard is responsible for enforcement of regulations governing the use of TWICs at MTSA-regulated facilities and vessels. The DHS Policy Screening Coordination Office serves as a coordinator in support of these efforts.

DHS's approach to TWIC has been to address immediate security needs while simultaneously building toward the end-state solution. Never before has the Federal Government attempted to conduct security threat assessments and issue a credential on this scale with such a geographically dispersed population of private sector workers. To meet this challenge, we had to plan carefully, consult, incorporate feedback, and adapt to evolving needs: our work is still ongoing.

TWIC Enrollment and Issuance

TSA began the national deployment of the TWIC program on October 16, 2007, with the enrollment of maritime workers at the Port of Wilmington, Delaware. A nationwide requirement for individuals to hold a TWIC in order to access MTSA-regulated facilities and vessels went into effect in April 2009, and TSA continues to operate approximately 135 enrollment centers in ports and in areas where there are concentrations of maritime activity throughout the United States and its territories.

Almost five years later, DHS has enrolled over two million TWICs to longshoremen, truckers, merchant mariners, and rail and vessel crew members nationwide. TSA-issued TWICs are visually inspected by port and vessel guards, for visual identity checks before a facility or vessel owner/operator grants unescorted access to secure areas. A visual inspection must include, at a minimum, a match of the photo on the TWIC to the individual presenting it; verification that the TWIC has not expired; and a visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

For the first time in the maritime environment, TWIC established uniform vetting of maritime workers based on recognized standards. These standards include a check for ties to terrorism, an immigration status check, and a criminal history records check. TSA conducts recurrent vetting

for ties to terrorism using the Terrorist Screening Database and other data to which only the Federal government has access. With TWIC, port security officers across the country encounter a single, recognizable, tamper-resistant credential, rather than hundreds of different identity cards, thus allowing them to make more informed access control decisions than was ever-before possible. TSA also created a canceled card list that is accessible by port and vessel owners and operators to inform them when a TWIC card has been revoked.

Security Enhancements

As of April 15, 2009, TWICs were required to be presented upon entry to MTSA-regulated facilities nationwide. This requirement provides a significant maritime security benefit by demonstrating to facility and vessel security operators that the TWIC holder, seeking access to a MTSA-regulated facility or vessel, has successfully passed the security threat assessment. The Coast Guard uses a scalable and progressive enforcement approach to ensure compliance, starting with on-site education and correction and elevating up to, and including, civil or criminal penalties.

The Coast Guard began supplementing its visual inspection activities with spot checks using hand-held card readers to ensure that workers' credentials are valid and that each identity is verified. The Coast Guard has deployed over 275 mobile readers that are capable of validating TWICs and other credentials during facility and vessel inspections and law enforcement boardings. Persons accessing secure areas of MTSA-regulated vessels and facilities are subject to electronic verification of their TWICs on a random basis using portable TWIC readers. To date, Coast Guard has verified approximately 220,000 TWICs using hand-held readers and visual inspections.

DHS has also pursued the re-use of security threat assessment results, where appropriate, to reduce costs for the TWIC holder. Based on public comments to the TWIC Notice of Proposed Rulemaking (NPRM), the 2007 TWIC Final Rule included the ability to provide a reduced fee for documented merchant mariners, as well as CBP's Free and Secure Trade (FAST) driver program members, and truckers with a hazmat material endorsement (HME) to their commercial driver's licenses.

TWIC Readers

The Coast Guard is in the process of drafting a NPRM for TWIC reader use, based on the results of the TWIC Reader Pilot, which was required by the SAFE Port Act of 2006 to be completed before the final rule.

DHS has been laying the groundwork for the rulemaking since separating it from TWIC enrollment and issuance. In 2009, the Coast Guard published an Advance Notice of Proposed Rulemaking (ANPRM) to describe its proposed risk-based framework and to solicit comments from the public. The ANPRM also described potential costs and benefits from the deployment of TWIC readers. In response, the Coast Guard received and considered approximately 100 comment letters in response to the TWIC Reader Advanced Notice of Proposed Rulemaking,

and comments received at the public meeting aligned into approximately 20 categories, which the Coast Guard used to inform its continuing development of the NPRM.

Concurrently, TSA conducted the TWIC Reader Pilot Program to support the development of the TWIC reader rule. From 2008 through 2011, TSA evaluated the technical performance of the TWIC biometric reader function at a sample population of maritime facilities. TSA was able to gather valuable data on reader performance, as well as assess the operational and business process impacts of conducting biometric verification of identity under diverse field conditions. A final report on the results of the TWIC Reader Pilot Program was delivered to Congress in February 2012.

Initial development and deployment of the pilot program among the TWIC reader pilot sites presented several challenges, and valuable lessons learned. From the outset of the pilot, for example, maritime stakeholders requested that card readers be capable of conducting a biometric match, without requiring the workers to enter their personal identification number or inserting their card into the reader.

Other challenges emerged in execution, due to the voluntary nature of the pilot, which allowed participants to proceed at their own pace. At some facilities, timelines for technical and physical infrastructure modifications were extensive and the government did not position itself to enforce a project plan. Furthermore, the recession had a tremendous impact on commercial operators, which meant reductions in staff and financial reserves across the board. This translated into real concerns from ports and facilities about matching grant funds in general, and specifically whether the grant funding received was sufficient enough to support technical and physical modifications. TSA offered general guidance to ports and facilities, but could not provide a “one-size-fits-all” reader template due to the unique nature of each regulated facility and vessel operation.

The pilot operation also highlighted security and operational benefits associated with readers including the automation of access control, so that regular users could use their TWICs for quick and easy processing into a port. In turn, participating pilot port security officers gained integrated access control systems resulting in more efficient and effective processing of workers entering secure areas.

Despite all the challenges associated with the pilot, several key factors were identified in the final report – such as business impact, technology, infrastructure requirements, environmental considerations, costs, and benefits – that could be incorporated into the TWIC reader rule. DHS anticipates that the TWIC reader rule NPRM will be published later this year. The Coast Guard will carefully review all public comments submitted through the docket and those received at any public meetings Coast Guard holds while drafting the final rule.

Recent Announcement

On June 15, 2012, DHS announced that beginning August 30, 2012, DHS will offer eligible TWIC holders the opportunity to replace their expiring TWICs with a three-year extended expiration date (EED) card for \$60.00. DHS is offering the three-year option to make the re-

enrollment process more cost-effective for eligible workers while the TWIC reader rule is still pending. DHS considers the EED card equivalent to a standard TWIC and will allow port and vessel operators to accept EED cards as they accept standard TWICs.

DHS is offering the EED TWIC option to make the re-enrollment process more cost-effective for those individuals who are U.S. citizens or U.S. nationals and whose TWICs will *expire on or before December 31, 2014*. Those TWIC holders who are not U.S. citizens or U.S. nationals or who are eligible but do not wish to use the EED TWIC option may renew their expiring TWICs by completing the standard enrollment process for a five-year TWIC, which includes an enrollment fee of \$129.75. The EED TWIC is a one-time temporary extension of the current TWIC; upon the expiration of this three-year EED TWIC, all TWIC holders will be required to enroll for a standard five-year TWIC.

Conclusion

Prior to the TWIC Program, there was no standard identity verification or background check policy for entrance to a port facility or vessel. This created vast opportunities for fraud and risk. Today, facility and vessel owners and operators look for one standard identification document that confirms the holder's identity, and verifies that he or she successfully completed a security threat assessment. TWIC cards contain security features that make the card highly resistant to counterfeiting. When biometric verification becomes a requirement and readers are in use, we will further enhance security at port facilities and vessels regulated by MTSA.

DHS and its partners have taken significant steps to add layers of security to protect our nation's port facilities and vessels. These steps link together information sharing, security, and law enforcement from across DHS and a multitude of partnerships. Each security layer builds upon and complements the others. TWIC is one of those layers. Thank you for this opportunity to update the Committee on this important link in DHS's maritime security strategy.