American Association of Port Authorities
Alliance of the Ports of Canada, the Caribbean, Latin America and the United States

1010 Duke Street
Alexandria, VA 22314
Phone: (703) 684-5700
Fax: (703) 684-6321
www.aapa-ports.org

TWIC IMPLEMENTATION TALKING POINTS
April 26, 2007

- TWIC is a major step toward further increasing the security of our nation's ports and making them safer.

- AAPA supports implementation of the Transportation Worker Identification Credential as the federal standard for authenticating the identity of those entering secure areas of U.S. ports and for barring entry to those who may be deemed a threat. Having a standardized TWIC nationwide is an important security protocol for U.S. ports to avoid a patchwork of conflicting local and state solutions.

- AAPA and its member ports are working cooperatively with DHS and its contractors with a goal of ensuring TWIC is rolled out effectively and efficiently. It is in everyone's best interest that TWIC implementation be carried out thoughtfully and with attention to detail to avoid any breakdown in security or efficient movement of goods and people through our ports.

- One of the key components to an efficient TWIC roll-out is for DHS to educate ports and their users about the upcoming program. This will help reduce confusion in obtaining TWIC cards, increase the likelihood for a streamlined implementation process and minimize the number of TWIC-related gate entry denials once the cards are issued.

- To reduce the potential for TWIC card denials based on an applicant's background, AAPA supports DHS's waiver system, which provides flexibility for non-U.S. citizens and applicants flagged by the background check to make a case as to why a particular individual is not a security risk and should be issued a TWIC. By looking at TWIC applications on a case-by-case basis rather than on rigid interpretation of the rules, AAPA believes this will help improve port security by focusing attention on applicants who are security risks.

- AAPA supported splitting the TWIC roll-out into two phases to allow more time to evaluate card reader requirements. Phase two of TWIC will require biometric card readers at port facilities to authenticate the identity of cardholders and positively tie each individual to the card they produce. DHS must develop technology standards that work in the marine environment. Thus, DHS should thoroughly test card readers first to ensure a smooth installation and use of this new technology. Card reader testing will further safeguard the security of our ports while helping ensure that the efficient flow of commerce and people are not unduly hampered.

- AAPA endorses the National Maritime Security Advisory Committee's recommendation that the TWIC cards and card readers utilize contactless technology in which TWIC

cards can be "read" without having to touch the surface of the reader. This will greatly increase the ease of use and diminish the potential for card and/or reader malfunctions. AAPA also endorses NMSAC's recommendation that the fingerprint template resident on TWIC cards not be encrypted. Because a template is not a fingerprint image, but an algorithm generated by reference points, it is of very little use to an identity "thief." These algorithms are currently unable to be reverse engineered into usable complete fingerprint images. It would be a lot more accurate and much less challenging to extract a useable fingerprint image from a car door, window, soda can or drinking glass. For this reason, encryption of the fingerprint template is not cost effective or security enhancing. It would simply add unnecessary costs, program administration and time to the transaction.

- The recent GAO report critical of the TWIC program suggests the program has been underfunded from the beginning and needs to have a higher priority in the DHS budget going forward. AAPA agrees.

- To comply with the TSA mandate that maritime facility operators know who is on their premises at all times, AAPA believes it should be optional and at the facilities' discretion to install TWIC card readers at exit gates. While AAPA supports access control for facility entrances, exit controls are costly and may provide very little extra protection of the facility.

- AAPA also opposes the proposed rule requiring use of a PIN at MARSEC III. Because of infrequent use, most workers are not likely to remember a PIN, and the biometric security protections in the card – digital photograph and fingerprints – are adequate security at all levels.

- The Port Security Grant program should allow grants to help pay for the purchase and installation of card readers and computer systems needed for TWIC. TSA has estimated that the cost to purchase and install card readers at U.S. port facilities would be about $300 million. This figure does not consider the cost for operation and maintenance, which would likely increase the cost of the card readers to about $1 billion for the first 10 years of the program. Furthermore, AAPA believes TSA's card reader purchase and installation estimate is too low because it does not take into account adding card readers at exit gates (should they be required), nor does it consider the costs for accompanying computer systems that must be installed, maintained and regularly updated. To help pay for card readers, AAPA supports the SAFE Port Act of 2006, which authorizes Congress to appropriate $400 million a year for port facility security.

- AAPA believes that ports and terminals that pose low security risks, such as grain and mineral bulk facilities, should be given the option to either install approved TWIC card readers to match the card carrier with the card, or use visual or other non-technological means to authenticate the card and carrier.

- AAPA supports background reviews and terrorist checks for all TWIC card recipients. However, many port operations rely on a temporary workforce to help unload a ship, and these "casual" laborers are given visitor or temporary passes to allow access. These are often not union workers, especially in areas other than the West Coast. The escort rules

as described in the proposed rule are impractical as applied to these types of workers and would result in added expense and inefficient terminal services. AAPA believes TSA should develop a way to quickly get these workers cards and background checks in order not to disrupt the workforce, similar to Florida ports.

TWIC IMPLEMENTATION BACKGROUNDER
March 30, 2007

(Please Note: The following AAPA summary of the TWIC implementation only relates to maritime facilities and not to vessels. *AAPA will send the DHS enrollment schedule for ports as soon as it is published. For additional reference, please see the TSA/DHS PowerPoint presentation, "Final Rulemaking Overview" at http://aapa.files.cms-plus.com/PDFs/TWIC%5Ffinalrule%5F04%2D16%2D07.ppt***)**

The Department of Homeland Security (DHS) will begin implementing the Transportation Worker Identification Credential (TWIC) regulations for maritime workers starting in May 2007. There will be a rolling implementation throughout the nation, based on a list (which has yet to be released) that will be developed by DHS. TWIC was mandated under the 2002 Maritime Transportation Security Act (MTSA) and the 2006 SAFE Port Act. The Transportation Security Administration (TSA) and U.S. Coast Guard are responsible for implementing and enforcing the regulations.

The TWIC regulations will be split into two phases. Phase one relates to the issuance of TWIC cards and will begin this month (March 2007). Card issuance will be done on a rolling basis, predicated on the timeline provided in the SAFE Port Act. That schedule dictates that the 10 highest priority U.S. ports, as designated by the Homeland Security Secretary, must begin issuing cards no later than July 1, 2007. The 40 U.S. ports that are next in order of priority must begin issuing cards by January 1, 2008, and all other U.S. ports must begin issuing cards by January 1, 2009. Mariners will have until September 25, 2008, to get TWICs. The DHS, however, may implement the TWIC card issuance process more quickly. DHS has estimated that card enrollment will be completed at all ports within 18 months. For the first 10 ports, DHS previously expected to begin issuing the cards in the March –May timeframe, but has temporarily delayed card issuance due to a host of factors, including:

- the decision to use the most advanced federal government biometric standard and, for the first time, apply it to the commercial sector;
- the need for TWIC to work anywhere in the nation's private port environment across companies and industries;
- TWIC's unparalleled flexibility and its massiveness in scale;
- the need for TWIC security checks to be integrated into all of TSA's vetting programs; and,
- the progress in addressing privacy and data management concerns identified by GAO.

TWIC phase two relates to card readers and other facility requirements. The final requirements for phase two have not been released. A second comment period for the reader requirements will take place, and a card reader pilot program will commence, before ports will have to install

readers. DHS may also provide an approved reader technology list for port facilities to use. The SAFE Port Act of 2006 requires regulations for facilities to become effective January 2009.

According to the phase one regulations, all MTSA regulated facilities must escort individuals who do not have TWICs. *(See escort requirements under Q&A section of this document.)* The TSA is responsible for issuance of most cards and the U.S. Coast Guard is involved in mariner and facility compliance. A contractor, Lockheed Martin Corp., has been hired for the TWIC enrollment process and is also using a subcontractor at Deloitte for stakeholder outreach. The Deloitte subcontractor will be providing information to employers to help educate workers about the new requirements and help establish the 130 enrollment centers.

Soon, DHS will publish a list of ports where the enrollment process will start. Once the enrollment center list is published, ports must notify their workers of the need to get a TWIC. Workers will then have at least 60 days to apply. Facilities will have their compliance date for limiting access to TWIC card holders tied to the completion of initial enrollment of the Captain of the Port (COTP) zone where the facility is located. This date will vary, and will be announced for each COTP zone at least 90 days in advance by a notice published in the *Federal Register*. Once this second notice on facility compliance is published, facilities must notify employees of this date.

Workers must provide biographic and biometric (photo and fingerprint) information to apply for a TWIC and will pay a fee of $137.25, although workers with current, comparable background checks (including a Hazmat endorsement on a commercial driver's license), merchant mariner document or Free and Secure Trade (FAST) credential, will pay a discounted fee of $105.25. This amount is below the estimate of $139 to $159 that the federal government had anticipated charging for the credential. Those requesting replacement cards will pay a reduced fee. Workers may pre-register on-line and then go to the enrollment center for fingerprinting and to have their photos taken. The TWIC review will include disqualifying criminal offenses, immigration status and mental capacity status. These checks will also determine if the person is on any terrorism-watch lists. Workers must return to the registration center to pick up their credential. The first version cards may also require some software changes once the final reader requirements are approved. TWIC holders will be required to return to the TWIC enrollment facility to make this change but there will not be a fee.

Lockheed Martin will establish the TWIC enrollment centers and will work with the ports to inform facility employees and customers about these centers. They will be cash-free facilities, allowing employer accounts, money orders and credit card payments, but no cash transactions. The turn-round time for issuing most cards will be 10 days, according to TSA.

On March 7, 2007, representatives of the TSA, Coast Guard and Deloitte Consulting, which is part of the Lockheed Martin TWIC Team, hosted an outreach meeting for area facility security officers at Wilmington, DE. Copies of some of the presentations from that session have been posted to the Delaware River Maritime Exchange web site and are available for download at http://www.maritimedelriv.com/Port_Security/TSA/TSA_Port_Security.htm.

To view DHS's April 2007 "TWIC Enrollment Port Brief," click http://aapa.files.cms-plus.com/PDFs/TWIC%20Enrollment%20Port%20Brief.pdf.

For a list of Lockheed Martin field coordinators, click http://aapa.files.cms-plus.com/PDFs/TWIC%20Field%20Coordinators.xls.

A map of the Coast Guard districts the field coordinators cover is available at: http://aapa.files.cms-plus.com/PDFs/FieldCoordvsCGDistrict%2Emap.pdf.

The Coast Guard has established a help desk for TWIC related questions. Call **202-372-1126** or email questions to **uscg-twic-helpdesk@uscg.mil**. For other policy related questions, contact: **TSA: 1-866-TSA-TWIC** or **credentialing@dhs.gov**.

The Transportation Security Administration's latest version of its TWIC FAQs is available at: http://www.tsa.gov/what_we_do/layers/twic/twic_faqs.shtm. AAPA has also developed a set of FAQs, which are printed below.

AAPA FAQs (March 7, 2007)

How does the criminal background check effectively guard against making TWIC cards available to potential terrorists? Similar to criminal background checks given to those who work in other critical infrastructure areas and professions where tight security is crucial, this is just one of several steps used to guard against enabling those who wish to do harm. TSA/DHS have set strict rules for obtaining a TWIC card, including that everyone must submit to a criminal background check, an intelligence/terrorist screening check, an immigration status check, and a 10-digit fingerprint scan. This is similar to the requirements for hazardous materials commercial truck drivers. *(See attached PowerPoint for full list of crimes).*

What will happen to workers who fail the background check? Workers who believe that they meet the requirements but have been turned down for a TWIC may pursue an Administrative appeal. Individuals who fail this appeal will only be allowed escorted access. Companies may need to relocate these workers to an area outside a security area of a facility.

Who will pay for the TWIC and will workers get paid for time for enrollment? That will be handled on a company-by-company basis.

How effective will TWIC be if facilities have not installed the reader technology? The TWIC includes a tamper proof photo as well as fingerprint biometrics. Facilities will have to ensure all individuals seeking unescorted access produce a valid TWIC card and then perform a visual check against the card. This visual check is a step-up in the nationwide security of ports. The card is highly tamper proof. To enhance security further, DHS will eventually require facilities to have automated card readers to verify the fingerprints. This technology has not been tested. The SAFE Port Act of 2006 required that DHS test this technology before implementation. The original TWIC pilot only tested the issuance and use of cards. Until the reader technology is tested and installed, U.S. Coast Guard will conduct random verifications of cards at facilities.

What will happen when a card reader can't validate a TWIC credential, either due to malfunction or improper use by worker? Is there some sort of back-up protocol to avoid congestion and gridlock? The TWIC regulations outline certain procedures and protocols to be

followed. We hope through use of good technology and education of those using the cards and those charged with verifying TWIC card validity that we can minimize gridlock. Some ports have already made major changes to entrances of regulated areas to better handle the flow of traffic and provide alternative routes for potential congestion issues.

Before TWIC card readers are installed, how will ports positively identify the card carrier as being the one to whom the card was issued? The card includes a tamper proof photo which a security officer can review. Also, a person must have a reason to be on port property– such as a laborer or a trucker – and the port must give the worker approval to come into the port. Having a TWIC does not provide automatic access to a port. You must have a business reason to be there.

What's to stop a terrorist from forcing a TWIC card carrier to escort him/her into secure facility? While no security system is 100 percent foolproof, port facilities all have procedures they must follow, depending on their individual facility security plan, to protect against illegal or forced access. Much of this is based on the observance skills and training of the security personnel charged with permitting secure port access. Furthermore, the Coast Guard may do random or "spot" inspections of vehicles and individuals entering the secure areas of port facilities. In cases where there is evidence or sufficient suspicion of criminal activity, the Coast Guard may also stop and search vehicles or individuals entering or leaving a secure port area. However, the primary responsibility for authorizing entry into secure port areas remains with the facility operator.

Are TWIC card costs tax deductible? They are tax deductible, as a business expense, if you qualify overall for the business expense deduction.

Will Florida port workers need both a TWIC and a FUPAC? TSA is currently working with Florida officials to see if the technology for both cards can be made similar enough that two different readers are not needed in Florida. All Florida port workers needing unescorted access to secure port facilities will have to get a TWIC because the final rule said no other card could be used as a substitute. Florida, however, could change its rules to not require the FUPAC card once TWIC goes into effect, but that will require a change in Florida state law.

Can I enroll for a TWIC on-line? You can pre-enroll on-line but you must go to the enrollment center to pay the fee, give your fingerprints, get your photo taken and return to pick up your TWIC.

What is the lag time between applying for a TWIC and getting the actual card, and is there a temporary card available in the interim? What happens if a worker loses his/her card between the time of card loss and reinstatement? New workers who are employees of owners and/or operators of facilities and have received TSA approval can gain "accompanied" access for 30 consecutive days (with an additional 30 days with COTP's approval) while waiting for their card to be issued. Others, such as longshore workers, cannot be granted "accompanied" access and must either be escorted, or wait until their card is issued to gain "unescorted" access. TSA says it expects the time between application and release of a TWIC will be 10 days. In cases where a TWIC is lost, stolen or damaged, the facility can give unescorted access up to 7 consecutive days. For lost and stolen cards, TSA estimates replacement cards will be issued in 3-4 days after the request is made, and there is a reduced fee to get the card.

What is the definition of "escorted" and "accompanied" access, and how are they different? DHS's regulations and proposed guidance outlines the term "escorted" and has two different requirements depending on whether the area is restricted or secure. Escorting is a performance standard and may be negotiated by each facility with the Coast Guard. However, the regulations outline the following recommendations: For secure areas, "escorted" means side-by-side accompaniment (1 TWIC to 10 escorted) or monitoring. Monitoring must enable sufficient observation of the individual with a means to respond if they are observed to be engaging in unauthorized activities or in an unauthorized area. In a restricted area, "escorted" means side-by-side accompaniment (1 TWIC to 5 escorted).

"Accompanied" access is a term reserved only for facility or owner-operator new hires. Because most longshore workers are not hired directly by facility- or owner-operators, most would not be granted "accompanied" access. New hires have limited access to secure facilities and do not need to be physically escorted as other non-TWIC holders do. However, new hires must be accompanied in accordance with the Coast Guard's draft Navigation and Vessel Inspection Circular (NVIC) guidance. That draft guidance defines "accompanied" access as only being available to new hires who are assigned to work units, or groups, of up to 25 employees, in which no more than 25 percent of the work unit employees are new hires. A work unit is a subset of the larger organization characterized by its geographical location and the extent of its operations, where employees work closely together on a regular basis. This proximity would facilitate accompaniment of a new hire. For example, a work unit may be a fire department on an oil refinery or a business office on a container facility.

What about the PIN requirement? Is that going to be enforced universally or just in MARSEC II or higher situations? The *TWIC Implementation in the Maritime Sector - Final Rule*, published in the *Federal Register* on January 25, 2007, defines Personal Identification Number (PIN) as "a personally selected number stored electronically on the individual's TWIC." The cards that will be issued initially will contain a PIN, per the requirements of the current technology standards (FIPS 201) being followed by the TWIC program.

Because the card reader requirement has been removed from this rule, the PIN requirement will not be an issue for routine access controls. It should be noted, however, that U.S. Coast Guard will be conducting spot checks for TWICs, using hand-held readers, and that if an individual is stopped during one of these spot checks, he or she will need to know the PIN in order to unlock the biometric stored on the card and allow for biometric verification.

It is not clear at this point whether the use of the PIN will be aligned with MARSEC II and higher. This will likely be clarified when the reader requirements are decided in the second rulemaking. The Coast Guard stated in the January 25 rulemaking that they will monitor issues with PINs during the spot checks, and if problems are identified, they will be addressed in the Notice of Proposed Rulemaking (NPRM) re-proposing the access control and reader requirements. AAPA and other maritime interests, including those comprising the National Maritime Security Advisory Committee (NMSAC), have opposed and continue to oppose any requirement that the PIN be used by facilities as part of the TWIC verification process.

What is the definition of "improper transportation of a hazardous material" as it pertains to

permanent disqualification from obtaining a TWIC? If I were cited for, say, carrying a can of gasoline in the trunk of my car for use in my lawnmower, would that permanently bar me from obtaining a TWIC, since gasoline is considered a hazardous material? To be permanently barred from obtaining a TWIC, you must have been convicted of a felony. You can ask the TSA contactor at the enrollment center about these detailed questions and ask for a waiver if you think your circumstance is unique.

How is it that "murder" permanently disqualifies someone from getting a TWIC, but "assault with intent to murder" doesn't? This is a policy question for DHS. The proposed rules may include some insights into why DHS selected certain crimes.

What is meant by "contactless" biometric? Does that mean a scan can be done without physical contact of the fingers or hand to a scanner? Many ports with access control systems today have "contactless" readers using wireless radio frequency (RF) technology. These are usually referred to as proximity cards and readers. To gain access, the user simply holds the card "in proximity" to the reader and the gate or door opens. In a "contactless" biometric scenario, the biometric data contained on the card can be read in this fashion. The card does not need to be swiped or touch the machine in any fashion. However, when a biometric verification is required (i.e. a physical fingerprint needs to be presented to see if it matches the data transmitted by card), the user will need to place his/her fingerprint on a sensor in order to capture that data. Currently, it is unclear at what MARSEC levels a fingerprint scan would be required. This will be addressed in the second USCG rule related to technology aspects of the TWIC.

Can anyone with a valid TWIC escort someone in a secure port facility who doesn't have a TWIC? DHS regulations only state that someone who has doesn't have a TWIC must be escorted by someone who does. Whether a driver can bring a passenger into the port who does not have a TWIC will depend on the individual facility security plan.

How long are TWIC cards good for, what is the cost for a renewal, and what security checks will be made for renewals? TSA's final rule says that TWICs are valid for five years from date of issue, unless renewed before the five-year term ends. The expiration will be displayed on the face of the credential. Renewals, which cost the same as the initial enrollment (similar to renewing a passport), must be requested in person at any enrollment center at least 30 days before expiration in order to initiate the renewal process. This will provide sufficient time for TSA to conduct a new security threat assessment and the Coast Guard to complete any review necessary to renew any required documents. Renewal applicants must provide the same biographic and biometric information and identity verification required in the initial enrollment. In a news release distributed on January 29, 2007, TSA said the Standard TWIC Fee will be $137.25, which is below the amount indicated in the final rule. The fee includes the cost for the threat assessment, program management, card production and issuance. *(For the Standard Enrollment, Hazmat/Mariner/FAST TWIC Enrollment and Lost/Damaged Card Replacement costs, see page 8 of the attached PowerPoint presentation.)*

How much will a replacement card cost if I lose my TWIC? The May 26, 2006, Notice of Proposed Rulemaking (NPRM) established the Replacement Card Fee of $36. However, TSA's later analysis showed that this fee actually costs out at $60, but TSA didn't include the $60 figure in the final rule due to the large difference in amount from the NPRM. TSA's final rule proposes

to change the Replacement Card Fee to $60, although a final determination hasn't been made.

If someone is convicted of a disqualifying criminal offense while holding a valid TWIC, is there a tie-in with local, state or federal law enforcement authorities that would notify TSA? Is there a procedure to pull their TWIC credential? Local law enforcement agencies report to their respective state law enforcement agencies, which generally report criminal convictions to the federal criminal database, but not all states do this consistently. TSA will periodically update its database on all TWIC card holders against the federal database, and under the original proposed regulations, facility operators would be required to check the TSA database at least once per week and compare it against their own. For more information on what happens to a valid TWIC card holder convicted of a disqualifying criminal offense, please check with any TSA call center.

# # #