

**National Maritime Security Advisory Committee (NMSAC)
Credentialing Workgroup**

April 25, 2005

TWIC Task Statement

I. TASK TITLE: Transportation Worker Identification Credential (TWIC) for use in U.S. port facilities and on U.S. vessels.

II. BACKGROUND: The Transportation Security Administration (TSA) and the Coast Guard are partnering to develop a joint rulemaking to implement the Transportation Worker Identification Credential (TWIC) for implementation in the maritime mode. The maritime TWIC will satisfy the domestic credentialing requirements of the MTSA, and significantly improve security on U.S. vessels and within U.S. ports. The primary goal of the program is to develop a nationwide transportation identity solution that verifies the identity of transportation workers, evaluates their background information to determine whether they may qualify for unescorted access to secure areas, and assists transportation facilities and vessels with controlling access to their secure areas. Additional benefits of the program include reducing the duplication of credentialing efforts and establishing uniform and consistent standards for identity management for all transportation modes.

III. PROBLEM STATEMENT: There is not an all encompassing maritime transportation worker identity verification and background check system currently in place. TSA and USCG intend to issue a joint rulemaking document that will outline various requirements and applicability for the TWIC. This rulemaking will have a major impact on vessel and facility access control provisions and on those maritime transportation workers who will be required to obtain a credential. The regulation will seek to achieve the security benefits that Congress expected when the Maritime Transportation Security Act was enacted without imposing unnecessary burdens on the regulated community. Comment is sought on the impacts and processes involved in a future TWIC program.

IV. TASKS: Provide comment on the following:

- For the purposes of the following questions please base your responses on the definition of a secure area provided in question #1. You may also address alternative definitions of a secure area for the follow-on questions.
- Attachment 1 provides an overview of the anticipated TWIC workflow. Please refer to Attachment 1 when addressing questions related to sponsorship, enrollment centers and card production.
- DHS plans to model certain aspects of the TWIC program on the program TSA now has in place for performing background checks on commercial drivers seeking hazardous materials endorsements. Those regulations include a list of disqualifying crimes, appeals and waiver processes. Please refer to Attachment 2 when answering questions related to background checks, appeals and waivers.

1. Section 70105 of the MTSA requires the development of a Transportation security card or TWIC, for individuals with unescorted access to secure areas within maritime facilities and vessels that were required to submit a plan to the Secretary for approval under Title 33 CFR Parts 104, 105, & 106. Please comment on the proposed definition of a “secure area.” The secure area aligns with the access control area provided in Part 105, or the outermost gate/entry point to the facility. For vessels, the secure area aligns with the entire vessel, and offshore facilities the secure area aligns with the entire platform.

Recommendation for inclusion in the Rule:

- a) That “secure area” should be defined in such a way as to coincide with the access control area determined by the facility operator in its security plan.
 - b) Given that the TWIC identity check will have been completed upon entry to the port facility, there is no need to require a worker’s TWIC to be read again to board a vessel. Vessel Operators, in accordance with their own plans, have implemented processes necessary to ensure the individual has a right to conduct business on or at the ship; from both security and practicality perspectives, it should not be necessary to read a TWIC each time an individual boards a vessel unless the vessel operator has created the requirement as part of the Vessel Security Plan.
 - c) TWIC should serve as the baseline requirement for unescorted access to a facility or vessel. Individual operators may elect to implement additional levels of security for access to their facilities or to areas inside their perimeters at their own discretion.
 - d) Possession of a TWIC will by no means guarantee access to a facility or vessel, or to a specific location within the site. The granting of unescorted access must be left to the individual operator; so too should the determination of who may be authorized to serve as an escort. Some operators may require their own security personnel be present to escort visitors, while others may grant this authority to their tenants who may also receive visitors or to other TWIC holders.
 - e) Access to Part 106 remote facilities that have limited access by off-shore vessels or helicopters can be controlled by having the TWIC card read at the point of embarkation.
2. Where should TWIC access points and biometric readers be located for facilities and for vessels? (e.g., at the gate, at the door, only at certain doors?) This question should be answered first from a security perspective and then from a cost/practicality perspective.

It is important to reiterate here that TWIC is not required to gain access to a facility but rather only to certain designated areas.

Recommendation for inclusion in the Rule:

- a) Accordingly, and consistent with the comments outlined above, the CWG recommends that the regulation does not stipulate specific reader locations.
 - b) In general, the location of the screening points should be as far away as practically possible from the point of potential damage. However, because the configuration of each vessel and facility is different, the individual operator should determine location and include this information in his or her security plan, which is then submitted to the Coast Guard for approval.
3. What is the estimated population of workers that may need to have a TWIC on a facility? What categories of workers—and roughly how many of each category (e.g. truckers, longshoreman, routine delivery/service personnel, marine/vessel operations services personnel, management/admin.) comprise this estimate? What other assumptions went into this population estimate, considering the definition of “secure area” and which facilities are included? What is the population of merchant mariners without documents or licenses that may be impacted?

Recommendation for inclusion in the Rule:

- a) The CWG cannot at this time approximate the total population of workers that may need to have TWIC cards on a facility. Individual members have provided their own estimates as outlined below, but the CWG encourages DHS to keep in mind that that these figures are only very broad assessments and may not necessarily account for the following:
 - Foreign nationals who may be included in the TWIC program;
 - Emergency response personnel;
 - Temporary or casual workers;
 - Vendors or contractors not directly transportation workers but who may need access to facilities or vessels; or
 - Employee turnover levels.

Estimates: The State of Florida estimates a population of 75,000 potential cardholders, but this figure does not include merchant mariners. The estimate for small passenger vessels is approximately 20,000 crew members and facility personnel. One company that operates U.S. marine terminals estimated that one of its larger facilities has 11,000 longshoremen, 10,000 truckers, 200 management staff, and 50 marine vessel service personnel.

Members have been asked to provide additional estimates or samples when possible. This information is due to the Coast Guard and TSA prior to 6 May.

TSA will share the information it has gathered regarding the overlap represented by individuals who would require TWIC cards for multiple modes (such as a truck driver who needs to enter a port facility) that will eventually all utilize the TWIC cards.

4. The intent of the employer sponsorship process is to provide an extra level of security in the enrollment process. What are the benefits and issues associated in incorporating such a sponsorship? Is this a process that would ultimately be beneficial for the program to incorporate? How would such a process ideally be implemented? How will the enrollment process be implemented to be most efficient and beneficial to the workers, facilities, and nation?

Recommendation for inclusion in the Rule:

A significant majority of the membership is opposed to the idea the sponsorship concept, and thus the CWG recommends that the TWIC program does not include a sponsorship component.

The group believes issuance of a card should be based solely on the individual's ability to meet the background check requirements. There are a number of reasons against requiring an employer to sponsor a TWIC enrollment application.

- a) An individual must be responsible for the TWIC application process from start to finish. Employers cannot be involved because of privacy and other important concerns. It is recognized that many applicants would need to sponsor themselves, such as the tens of thousands of owner-operator truck drivers and other service workers. Self-sponsorship will need to be allowed and this ensures that the system is "open." Sponsorship creates a closed system. Further, if the employer's role were for enrollment only with no further responsibility, sponsorship would not provide added security benefits.
- b) Sponsorship would add layers of bureaucracy to an already complex credentialing program. There is a large turnover in maritime worker workforce. If the worker needs a new TWIC every time he or she changes employers, immense complexities would be added. Further, if a new TWIC is not required when a worker changes employers, there seems to be little point in including an employer sponsorship. For example, does the fact that ABC Co. sponsored Worker A at one time make him less of a security risk when Worker A seeks to work for XYZ Co.? Additionally, as the TWIC and MMD are to be merged into a single credential, sponsorship would reinstate the discarded practice of requiring seafarers to obtain employer sponsorship.

- c) The background check and credentialing process will determine if a worker is a transportation risk, not whether he can find someone to sponsor him for enrollment.
- d) Many employers will require a TWIC as a condition of employment application. Making the employer become a sponsor will slow and encumber the hiring process, and delay putting qualified people to work.
- e) Liability issues arising from sponsorship are unclear.
- f) It is important to keep in mind that a TWIC does not entitle the holder to access. Each facility will still have its own criteria for determining if the TWIC holder has a legitimate need to be on its premises.

Minority Report

Some members believe having an employer sponsor is a critical component of the program. Primarily, the rationale for including a sponsorship component of the TWIC program is that it helps significantly in the establishment of a legitimate business necessity to enter a facility or area, can serve as the starting point for card issuance, and can be viewed as the first layer in securing the integrity of the program. Another advantage of the sponsorship component is that it allows for TWIC pre-enrollment, thus avoiding long lines at enrollment centers.

However, there are concerns that if a sponsorship is incorporated, it must be clear that the ultimate responsibility for obtaining a card lies with the individual, with the sponsor only providing validation. Although DHS should not attempt to dictate whether a sponsor organization has legitimate business at the port/vessel, there should be a mechanism to validate the organization (e.g. is it a business or a non-profit, how long operating, what is the nature of the business, who are the principals).

The rule would need to specify what the sponsor is entitled to know if an application is denied.

5. Please review attachment 2 and comment on whether you believe this would be appropriate for the TWIC program. What are the key processes of a waiver program for an individual found to be otherwise ineligible? Provide comment on alternative security arrangements that an employer might establish for an individual seeking a waiver?

Recommendation for inclusion in the Rule:

- a) The CWG recommends that the HAZMAT rule in attachment 2 be utilized as the beginning point for the requirements and disqualifying offenses. The Group qualifies its recommendations by noting the following:

1. Does permanent disqualifying offenses mean that in fact there is not a waiver for those offenses?
 2. With only ten crimes on the list, all of which are felonies, the Work Group requested that the attorneys at TSA provide an explanation of the waiver portion of the HAZMAT rule.
 3. “Employer” is an inconsistent term utilized in the MTSA, which was drafted in advance of the Coast Guard regulations for maritime security and the ISPS Code. Neither the Coast Guard regulations nor ISPS Code puts an onus on an employer for assisting individuals in obtaining waivers from anticipated government credentialing requirements. Thus, any reference to employer involvement in the waiver process is improper. Employer involvement is also inconsistent with issues involving the privacy rights of the TWIC applicant, and it may lead to inconsistent results and abuse. This recommended position is consistent with the Working Group recommendation that individual TWIC applicants maintain control of the applicant process from start to finish.
 4. Include language under number 6 of the Hazardous Materials regulation: Improper transportation of a hazardous material under 49 U.S.C. 5124 or a State law that is comparable where there is criminal intent by a person to alter, remove, destroy, or otherwise tamper unlawfully with (1) a marking, label, placard, or description on a document required by regulation prescribed under this chapter; or (2) a package, container, motor vehicle, rail freight car, aircraft, or vessel used to transport hazardous material.
 5. Request TSA attorneys review the language in 5 under the Hazardous Materials regulation. In #5, clarification of the criminal language is required. CMDR Stowe and Gary Fischer of TSA agreed to provide clarification of the offense enumerated in #5.
- b) There is no intent to put anyone out of work who is currently employed and does not pose a security threat based on security threat analysis conducted by TSA. Due consideration should be given to the impact on labor and their livelihoods.
- c) DSH should adopt a “limited term waiver” to the effect that if an individual is employed on the date of implementation, and is not otherwise a security threat as determined by a security threat analysis conducted by TSA, he should not be a position of losing his job due the requirement of obtaining a TWIC. This “limited term waiver” refers to the limited time available for application of the waiver and it is understood that the waiver would be for current employees only. It must be obtained within one year from the date of the implementation of the TWIC.
- d) For those who may have a past disqualifying act but are otherwise eligible under the limited term waiver provision, the language of the MTSA suggests some form of employer involvement in the waiver process. However the regulations expressly prohibit employers having access to the specific details

of the background investigations. As such, any employer involvement in the waiver process would be inappropriate. This interpretation is consistent with the HAZMAT CDL endorsement waiver procedure already in regulation and recommended by the Working Group.

- e) All new hires would receive a TWIC card after a fingerprint and name based criminal history check and security threat analysis conducted by TSA. The extent of the background check would be based on the fingerprint identification and a search would include the federal database. In addition to the federal criminal records check, a check of the state of residence criminal history would also be made. Again, the CWG is concerned that individuals would “shop” for a preferred state of residence if each state has different standards for threat assessment of terrorist activity.
 - f) It was agreed that in situations where an applicant has plead *no lo contendere* or where an adjudication was withheld that this be treated the same as a conviction. This rationale would set one standard to consider these situations as each court, each prosecutor, and/or each state criminal jurisdiction will have differing legal predicates for such findings and there is not one federal standard for these legal standards.
 - g) It was strongly held that it becomes unwieldy to have individual states with particular standards other than the national standards, effectively turning the card into a state card rather than a national card. In that vein, it was stated that the state of Florida is adamant that no national standards would be acceptable to Florida that are not at the same level or higher than those currently being maintained in Florida. If the final TWIC rule does not equal or exceed the existing State of Florida standard adopted and implemented since the year 2000, the result will be the lowering of public safety and protection at Florida’s 14 deepwater seaports.
6. Provide comment or considerations on the type of biometric to be used, if any, besides fingerprints and explain purpose. (From a cost/infrastructure perspective, i.e., procurement, installation, user-friendliness, familiarity, comfort level, etc.)

Recommendation for inclusion in the Rule:

- a) TWIC must include the individual’s digital photograph, and the CWG suggests that DHS adopt the similar standards for all national and international programs, such USVISIT and FAST.
- b) Because the environment within which many maritime workers operate is different than that of other transportation workers or alien visitors, the CWG recommends that the type of biometric to be used should be re-evaluated after completion of the Prototype phase of the current TWIC pilot program.

7. Provide comment on a federally managed approach versus a federally regulated approach. The “federally managed program” is a combination of federal oversight of outsourced contracts for the core system components and a companion rule that regulates a user fee and compliance. Under a federally managed program, the federal government would oversee the enrollment, verification of identity, and the issuance of the credentials. The “federally regulated program” would use a rule to regulate industry compliance to implement one or more core system components. Under a federally regulated approach, the federal government would mandate that industry must enroll port workers and issue credentials based on a federally conducted background investigation.

Recommendation for inclusion in the Rule:

- a) While there will be a regulation governing TWIC application, issuance and usage under either scenario, the TWIC program must be federally managed.
 1. In addition to the fact that the Congress’ intent under the MTSA mandates that the federal government manage this credentialing program, it is evident that the benefits of a federally-managed system far outweigh those which may be derived from one which is implemented under regulatory standard or guideline.
 2. First, a federally-managed program will protect collective bargaining agreements, and take the employer out of the potential employee grievance process.
 3. Additionally, in as much as states are moving toward uniform drivers’ licenses, a federally-operated transportation worker credentialing system will better ensure uniformity of the enrollment, application review, card production and issuance processes.
 4. It will help ensure adequate and appropriate resources are available to conduct the necessary checks, protect the sensitivity of the biographic and biometric information required for application, and limit the potential for security compromises or other integrity issues.
 5. From a practicality standpoint, there is also significant card production and issuance cost savings associated with a centralized, federally-managed program.
 - b) TWIC should utilize public agency trusted agents and other public agency partnerships; DHS can effectively structure and manage the TWIC program so as to best capitalize on existing business processes and infrastructure without expending duplicative resources to implement and maintain the program.
8. Who should enroll individuals (take biographic and biometric data)? Who should issue the credential after DHS vets the individuals and determines that they are eligible? What advantages and disadvantages are associated with each option?

Recommendation for inclusion in the Rule:

- a) In any discussion of enrollment, it is imperative that speed of process be a key factor in the decision process. As a result DHS should provide as many enrollment centers as practically possible, staffed by either DHS personnel or adequately trained trusted agents.
 - b) These trusted agents should be federal, state, or local public safety employees with specific security training.
 - c) TWIC is a public program that relates to defense of the homeland, and as a result activities associated with authorizations under the program should fall to those who have a fiduciary public safety duty. Further, in order to protect the sensitive data collected during the application process, the federal government must have ultimate responsibility for enrollment and issuance. Trusted agents must be subject to a higher level of scrutiny than are TWIC applicants; not only should trusted agents be held to the highest standard established for security background screening, the trusted agents should undergo financial and credit screening as well.
 - d) DHS should take advantage of opportunities to streamline the enrollment process by allowing pre-enrollment through secure Internet connections or existing facilities. Using existing infrastructure will make the most effective use of available resources. However, it should be noted the CWG has reservations about the idea of non-safety related agencies or organizations becoming involved in this process. DHS should first look to its own agencies, such as Coast Guard License Issuing Centers, or other federal, state or local public safety offices to process enrollments before seeking partnerships with agencies with non-security missions.
 - e) The CWG applauds the pre-enrollment process included in the current TWIC pilot program and recommends this be maintained upon TWIC implementation. Applicants can provide their basic demographic data a through a dedicated kiosk or secure Internet connection, thus dramatically minimizing the amount of time spent at the enrollment centers. This method not only helps decrease the potential for errors in application but also provides a third layer in the employee identification process.
 - f) Card issuance and distribution should be centralized to eliminate risks associated with storage of issuance technology and products (blank PVC and holograms) at various locations. With a strong background and screening component, TWIC could become a highly desirable commodity for someone seeking to do harm.
9. What should the cost be to the worker/employer? Who should pay for the TWIC? The individual? The individual's employer?

Recommendation for inclusion in the Rule:

- a) Individuals, such as those holding HAZMAT credentials, who have been screened to an equal or higher standard than the TWIC should not have to pay again to undergo a background check. They should not be penalized by having to pay for multiple applications, card issuance and background check fees. Rather, these individuals should be issued a TWIC having a five (5) year expiration date.
- b) The individual applicant is responsible to pay the fee at the time of application. Any potential employer reimbursements or other business relationships should not be defined in the regulation.
- c) TSA was authorized to levee a user fee for the credential and should collect only those direct costs for the program.
- d) The cost for the TWIC should be standardized at all enrollment centers.

10. Provide comment on the period of validity of a TWIC?

Recommendation for inclusion in the Rule:

- a) The TWIC should be valid for a period of five years, unless revoked for cause, which is consistent with many other programs. This recommendation assumes there is a regular sweep of the database – not less than annually.

11. Provide comment on a staggered phase-in process for the TWIC. If a staggered phase-in approach is used, how should the phase-in be structured? (geographically, by category of worker, etc.)?

Recommendation for inclusion in the Rule:

- a) Regional or geographic implementation of the phase in approach is most advantageous.
- b) A deadline established by TSA should be identified, with a timeline for the phase in implementation. The final implementation/compliance date should be consistent across the country and provide sufficient advance lead time to allow stakeholders to prepare.
- c) DHS should utilize foreign facilities with a Coast Guard presence to facilitate the Merchant Mariners' ability to apply.

12. Provide comment on requiring a TWIC for individuals with access to sensitive security information or other persons engaged in port security activities.

Recommendation for inclusion in the Rule:

- a) TWIC should be used as identification credential alone, linking an individual to a background check to a credential.
 - b) Using TWIC as a requirement for access to SSI appears to be outside the scope of the program and thus inappropriate.
 - c) Nor does there seem to be a specific link between holding a TWIC and SSI needs. Some individuals, such as foreign ship masters, for example, may need access to SSI, but may not be TWIC holders. SSI is need-to-know based on a certain situation at a certain time, and the TWIC can not be used to determine whether the individual meets the current criteria.
13. Provide comment on any other aspects of a TWIC program you wish to consider, and provide any further recommendation that will assist the TSA and the Coast Guard in this endeavor.

Recommendation for inclusion in the Rule:

- a) The process must be coordinated with other federal programs to avoid duplication and conflicts.
- b) DHS must develop and adhere to a reasonable schedule of program development and deployment. The original TWIC pilot program deadline date was December 31, 2003; this date has been postponed on multiple occasions, resulting in substantial cost increases to both industry and taxpayers, as well as delaying one of the most critical components of the overall homeland defense strategy.
- c) During the development of the TWIC pilot program, DHS needs to dramatically improve communications with TWIC stakeholders. On many occasions, the TSA made program and schedule changes without informing its pilot program stakeholders, or made technical or operational decisions (e.g., the design of the pre-enrollment web interface) without seeking the input of many of the pilot program participants. While we understand the many challenges TSA faces in implementing the TWIC program, there is little doubt the agency will save both time and money by working more closely with stakeholders during the pilot program; this will ultimately result in a stronger, more effective program upon deployment.
- d) Allowing for stakeholder participation in the rulemaking process is essential to the successful outcome of the program.
- e) TWIC should incorporate components of other programs, such as the MMD, wherever possible to eliminate requirement to carry multiple cards for

various purposes. Stakeholders should be invited to work with DHS to explore opportunities to best utilize the capabilities of the TWIC for these purposes.

- f) The issuance of TWIC must be a timely process, allowing workers to get to work, or it will not be successful. We also need to think about procedures for replacement of lost or stolen cards, as well as penalties for persons fraudulently obtain or use/attempt to use a TWIC.
- g) We have questions regarding the system to be used to communicate information from the government when a TWIC holder is subsequently found to present a sufficient risk to be denied further access. For example, if a TWIC is properly issued to an employee, but subsequently that individual is placed on a terrorist list or shows up in a criminal database, what information is sent to the employer and the terminals where the facility is granted access? How is the information shared? What is the process to follow if that employee now arrives at another facility seeking access? Is the facility supposed to apprehend this individual? Communicate the attempted access to local law enforcement but let him go? Etc.

V. ESTIMATED TIME TO COMPLETE TASK: Provide comment within 30 days of the tasking.

VI. TSA & CG REPRESENTATIVES:

Transportation Security Administration

Mr. John Schwartz
TWIC Project Manager
202-227-2177
john.schwartz@dhs.gov

Coast Guard

CDR Cyndi Stowe
Chief, Vessel & Facility Security Division
202-267-4150
cstowe@comdt.uscg.mil