



Kendra L. Martin
Director, Marine, Security & Corporate Affairs

1220 L Street, NW
Washington, DC 20005-4070
USA
Telephone 202-682-8517
Fax 202-682-8207

Email martink@api.org
www.api.org

Delivered via electronic mail

July 6, 2006

Docket Management Facility
USCG-2006-24196, TSA-2006-24191
U.S. Department of Transportation
Room Plaza 401
400 Seventh Street, SW
Washington, DC 20590-0001

Re: Docket # TSA-2006-24191, USCG-2006-24196

Attn: Docket Clerk:

API is pleased to provide comments on the May 22, 2006 Federal Register Notice of Proposed Rulemaking (NPRM) requesting comments on Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector [USCG-2006-24196, TSA-2006-24191]. API is a national trade association representing over 400 companies involved in all aspects of the oil and natural gas industry including exploration and production, transportation (marine and pipeline), refining and marketing. As such, our member companies have a direct interest in maritime security and in the proposed TWIC Program.

Because of API's historical involvement in maritime security activities and due to the significant impact the proposed requirements will have on our industry, API is pleased to provide comments on the United States Coast Guard's (USCG) and Transportation Security Administration's (TSA) NPRM on TWIC Implementation in the Maritime Sector.

API and its members remain steadfast in our commitment to protect our oil and natural gas infrastructure. We continue to strive to bolster our ongoing partnerships with federal, state and local authorities and to share security best practices with our counterparts in energy, transportation, and other critical infrastructure sectors. It is in this spirit of partnership that API stands ready to support the USCG and TSA to further secure our critical infrastructure by helping to identify and preclude those who pose a security threat from gaining unescorted access to secure areas. Such a stance will help ensure that energy supplies reach the U.S. marketplace safely and securely.



Given our mutual goal of protecting critical infrastructure, we want to ensure that the proposed TWIC program is implemented in a fair, business-like, and cost-effective manner. The following comments reflect our concerns and proposed recommendations and are listed in priority order.

Identification of System Specifications - Interface with Legacy Access Control Systems

In the “Development of TWIC Process” section, it states that all of the significant components of the TWIC system align with the Federal Information Processing Standards Publication 201 (FIPS 201), but there is no mention of the specific components of the TWIC system. API is concerned that this lack of technical specificity in the NPRM precludes the ability of industry to have adequate lead time in planning capital budgets for the implementation of the desired TWIC system configuration, to develop a migration plan and ensure maximum compatibility with legacy access control systems. More information is needed to fully understand what modifications are required to interface with the TWIC system. API respectfully suggests that more technical specifications be included in the Final Rulemaking.

Recurring Unescorted Access

In the “Definitions” section of 33 CFR 101.105, “Recurring Unescorted Access” means authorization to enter a vessel on a continual basis after an initial personal identity and credential verification, as outlined in the vessel security plan.” API recommends that this definition be modified to include facilities. We also recommend that on a random basis (commensurate with existing USCG-required screening rates for personnel and vehicles) select individuals be processed through biometric readers during MARSEC I. Once these individuals have had their biometrics checked at MARSEC I, they should not have to be processed through a biometric reader again until MARSEC II. At MARSEC II, all unescorted personnel entering or exiting a secure area should be required to use biometric readers for each entry and exit. At MARSEC III the same procedures should apply as MARSEC II with the addition of using a PIN. This approach recognizes existing legacy access control systems and incorporates a random screening process. It also recognizes that employees may have to enter and exit a facility through different gates multiple times during the course of a day.

Frequency of Updates from TSA Database

The NPRM states that the owner/operator will verify that an individual’s TWIC is valid, either by directly interfacing with the TSA system or by using a list of invalid credentials downloaded from TSA. According to the proposed text in 33 CFR 105.255(f)(1) and 33 CFR 105.255(g)(1), the validity of a TWIC presented for unescorted access shall be verified using information that is no more than seven (7) days old in MARSEC I and no more than one (1) day old for MARSEC II. API recommends that this text be revised to verify information that is no more than thirty (30) days old in MARSEC I, verify information that is no more than seven (7) days old in MARSEC II, and verify information that is no more than one (1) day old in MARSEC III. This modification will provide significant administrative relief for our facilities without causing

deleterious impacts on their security posture. Accessing the TSA database on a daily basis could stack personnel outside the gate which then becomes a safety concern for facilities and vessels alike. Our recommended modification is consistent with the USCG's maritime security directive to increase screening rates of personnel and vehicles based on increased MARSEC Levels. Screening rates do not reach 100% until MARSEC III. API is seeking a commensurate rate of increase for obtaining updated information from TSA. We also have concerns about the reliability and availability of TSA's database when every MTSA-regulated vessel and facility is seeking to update its TWIC Card access list. We need to understand how TSA will address the potential loss of their TWIC database as well as what our responsibilities will be in this worst-case scenario.

Access Control Processing Time

API is concerned about the access control processing time for employees and visitors that use the proposed TWIC card reader system. Under the best of circumstances, it will double the time it currently takes to process each individual seeking to enter and exit a facility. For large facilities that have high volumes of vehicle and pedestrian traffic, this processing time will cause significant operational delays during shift changes and peak truck loading and unloading periods. Some of our member's waterfront facilities experience several hundred truck and other vehicular visits per day.

Durability of Card Reader System

API is concerned that the approved TWIC system configuration and equipment will not withstand the harsh marine and industrial environments that characterize offshore platforms and waterfront facilities. We recommend that some system configuration and equipment flexibility be permitted to allow for contact-less card reader systems. These systems should be more durable and have less down time when operating in extreme hot and cold temperatures, salt air, and industrial environments. Furthermore, contact-less card systems should be able to handle higher volumes of employees and visitors at large refineries and other critical infrastructure sites than the technologies recommended in FIPS-201.

Implementation Schedule

In the "TWIC Process" section, it states that TSA and USCG are contemplating implementing a flexible rollout, with anticipated dates to be announced by notices published in the Federal Register. The NPRM indicates that facilities will have 12 to 18 months from the date the Final Rule is promulgated in the Federal Register to operate under the TWIC Addendums. API is concerned that this timeframe will be overly aggressive for the implementation of TWIC. As noted above, industry needs time to adequately plan, budget, and install the new TWIC system. Capital budgeting and project planning typically requires a three-year lead time to develop specifications, draft engineering drawings, identify qualified vendors, procure hardware and

schedule installation time in tandem with other competing safety, security, and operational projects.

API is also concerned about the availability of hardware for purchase when the regulations are published. According to the USCG and TSA, there are over 14,000 MTSA-regulated facilities and vessels that will be required to install TWIC-enabled systems. Most, if not all of these sites, will require multiple TWIC card readers and supporting infrastructure. The subsequent spike in demand for this hardware after the Final Rule is published will invariably cause a significant delay in the systems' installation nationwide.

Federal Preemption

The "Federalism" section of the NPRM says, "States would not be preempted from instituting their own background checks or badging systems in addition to the TWIC." We respectfully disagree with this approach. This will cause unnecessary duplication of effort, result in additional costs that must be borne by industry, not improve security, and could result in interference with interstate commerce.

Federal preemption is necessary for the same reasons that hazardous material transportation (HAZMAT) regulations are necessary. The HAZMAT regulations preempt states, cities, and local municipalities, from preventing the transportation of HAZMAT through their jurisdiction. Thus, the HAZMAT regulations allow interstate commerce to occur between the states and the approximately 30,000 local jurisdictions. Without this preemption commerce would come to a halt.

Similarly, a state, or local municipality's worker-credentialing criteria could be so intentionally onerous that certain activities could be completely prevented from occurring at ports in their state. For example, if a municipality decided that they didn't like a certain hazardous material; they could write the credentialing criteria such that a special background investigation was required for accessing that facility. Thus interstate commerce would be negatively impacted. The USCG should assert its preemption authority to prevent states from instituting their own badging and credentialing systems in addition to the TWIC.

Allowing different credentialing criteria for each jurisdiction is inefficient and ineffective. A company should not be expected to meet different credentialing criteria for each state simply because they operate in different states. For example, if a company has a facility in Louisiana and in Texas but each state has its own credentialing requirements, the operator would not be able to transfer an employee across state lines without getting a state credential. Further, if a pipe fitter works at a turnaround in a Louisiana refinery and then goes to work at a turnaround in Texas, he could find himself not able to cross state lines to apply his trade because the two states may very well have different credentialing criteria.

We also recommend that every state's law enforcement database populate national databases maintained by the FBI so that TSA can better vet applicants for TWIC Cards. Without this input, disqualifying applicant information from non-participating states will not reach TSA.

Notifying Employers on Personnel Denied a TWIC Card

As noted in the NPRM, TSA proposes to notify the applicant's employer if TSA determines that the applicant poses a security threat, and where appropriate, when issuing final determinations of threat assessment or immediate revocations. API strongly recommends that information pertaining to the denial of a TWIC card be shared with employers so that they can make a determination on whether or not to retain the impacted individuals, or transfer them to less sensitive areas. In API's letter dated May 17, 2005 to Mr. John Schwartz, TSA, and Commander Cyndi Snowe, USCG, it was stated that an employer should be given notification of the reason for denial of the TWIC. And that without this information the employer could be subject to a negligent hiring or retention lawsuit. The referenced letter conveys our position in more detail and is attached and submitted as part of these comments. API members need to know if the disqualifying information portends a security problem for their facilities and their personnel.

Processing Lead-Time for New Hires and Contractors

In the "Proposed Rule" section of the NPRM, it states that "owners/operators must provide applicants enough lead time to enroll so that TSA has sufficient time to complete the security threat assessment and issue the credential before the access control procedures go into effect... owners/operators should give individuals at least 60 days notice to begin the process. TSA cannot guarantee that any threat assessment can be completed in less than 30 days..." API is concerned that the 90-day lead time poses a significant problem for facilities in their ability to hire new employees and contractors on short-notice. Moreover, it will require facilities to add more security personnel to escort new hires and contractors until they receive their TWIC cards. Both of these factors will create major impediments for maintaining critical production and transportation infrastructure and expanding capacity at legacy facilities to meet the nation's growing demand for energy.

Definition of Secure Area

According to the "Definitions" section in 33 CFR 101.105, "Secure Area" means the area on board a vessel or at a facility or outer continental shelf facility over which the owner/operator has implemented security measures for access control, as defined by a U.S. Coast Guard-approved security plan. That definition essentially means that the entire MTSA-regulated facility is considered to be a "Secure Area." API does not understand why the new regulatory term – "Secure Area" – is being introduced three years after the implementation of MTSA regulations. Our preference is to have TWIC regulations apply only to Restricted Areas so that we can have unescorted access to Non-Restricted Areas of our facilities (unless our USCG-approved Facility

Security Plans dictate otherwise). By limiting the application of TWIC regulations to Restricted Areas, we will be able to focus our security efforts on those key assets that are critical to facility operations. Conversely, it will not impose unnecessary burden on portions of facilities that are not critical to the safety and security of operations (i.e. office buildings and other non-marine related portions of the facility).

Definition of Escort

In the “Definitions” section of 33 CFR 101.105, “‘Escorting’ means ensuring the escorted individual is continuously accompanied or monitored while within a secure area in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.” API recommends that this term be more clearly defined. Our preference is to identify various options for owners and operators ranging from one-on-one escorts to “zone defense” escorts whereby one or more escorts monitor the activities of multiple employees, contractors and visitors within restricted areas. This would greatly mitigate the cost and disruption to operations without having a detrimental impact on the effectiveness of the facility’s security program.

Enrollment Centers

In the “TWIC Process” section, it states there will be approximately 125 locations covering 300 ports where TSA plans to enroll applicants. These enrollment sites will initially be located in areas that are considered critical and have the greatest number of individual applicants. API is concerned that the processing infrastructure at fixed enrollment centers will not be adequate to address the influx of applicants from highly industrialized areas covered under MTSA such as Houston, Los Angeles, New Orleans, Philadelphia, and New York/New Jersey. We believe a fixed enrollment center supplemented by mobile enrollment centers at large facilities (e.g. refineries) will enable more efficient enrollment of personnel during the initial implementation phase. Ideally, mobile enrollment centers should schedule visits to each large facility to expedite TWIC Card processing and to minimize operational and economic impacts on facilities and neighboring communities.

API welcomes the concept of having mobile enrollment centers, but has concerns over the frequency of visits to remote sites. Many of our member facilities are located away from major metropolitan areas and will be at a disadvantage for enrolling their employees and contractors. API would like further clarification on the criteria for determining the visitation frequency for remote locations. Since applicants need to visit enrollment centers at least twice, we recommend that mobile enrollment centers return to initial enrollment sites multiple times so that enrollees can conduct their business, as needed.

Trusted Agents - Industry

As noted above, API is concerned about the influx of applicants seeking to obtain TWIC cards

when the Final Rule is published, and when fixed enrollment centers are established. API believes that the operator of the facility should have the option to function as the trusted agent for the enrollment of its (and only its) employees and contractors at that site. Industry facilities would use TSA-approved hardware, and use the same processing protocol, and vetting of trusted agents to operate enrollment sites that are proposed in the NPRM. We believe this option will fast-track the TWIC card processing period, maintain the same security, and minimize the time and costs of having personnel obtain cards off-site.

TWIC Card Requirements for State/Local Agencies and First Responders

Per 33 CFR 101.514, federal officials are not required to use a TWIC. API respectfully suggests that all Federal Personnel (USCG, CBP, ICE, etc.) present a FIPS 201-compliant ID card that can be validated. API agrees with the proposed text that “Law enforcement officials at the State and local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas.” We recommend that this provision be extended to other organizations responding to an emergency, namely fire departments, EMS, and mutual aid associations. Under the Incident Command System, first responders will be accounted for during an emergency. When prolonged incidents evolve into recovery and restoration activities, then emergency personnel should be escorted through secure areas, unless they too possess TWIC cards.

Eligibility of Individuals in Lawful Nonimmigrant Status

As stated in 49 CFR 1572.105 (3)(i), “An applicant applying for a security threat assessment for a TWIC or HME must be an individual who is in lawful nonimmigrant status, and possesses valid evidence of unrestricted employment authorization.” This appears to restrict nonimmigrant workers in H1B (visas issued to aliens who work temporarily in the U.S. in specialty occupations) or L1 (visas issued to managers and executives who transfer from a company’s foreign branch or subsidiary to a U.S. branch) status since they do not have unrestricted employment authorization. Many of API’s members have workers in this status. Ideally, we would like to have H1B and L1 employees eligible for TWIC. We respectfully seek clarification on this issue.

Prescribed Locations of Card Readers

We agree with the National Maritime Security Advisory Committee Credentialing Work Group’s (NMSAC CWG) position that owners/operators should determine where readers are located based on the security plan and the performance standards established in the NPRM. It is important that the government’s technology requirements allow maximum flexibility in the siting of card readers to bolster security without having a negative impact on critical operations. For example, some facilities may need portable biometric readers to supplement fixed readers for personnel entering during peak periods. If prescriptive regulatory language is used, then portable card readers may not be an option for facilities and vessels under this aforementioned scenario. For Outer Continental Shelf (OCS) facilities regulated under MTSA, we recommend that



owners/operators be permitted to have readers located at the point of embarkation on the platform and/or at the shore-side support facilities (heliports, crew boat/offshore supply vessel homeports).

Financial Impact on Contractors

API is also concerned that this program will be cost-prohibitive for some industry contractors, especially those that must travel from remote locations to fixed enrollment sites. We hope that the presence of mobile enrollment centers at remote locations will be able to provide travel relief for these contractors.

Thank you again for the opportunity to provide input into the development of this important program. API and its members are eager and ready to assist the USCG and TSA in this and all other security endeavors. If you have questions regarding the information offered or would like additional assistance, please don't hesitate to contact me at 202-682-8227 or searlesp@api.org.

Sincerely,

A handwritten signature in black ink that reads "Kendra L. Martin". The signature is written in a cursive style with a large initial "K".

Kendra L. Martin
Director, Marine Security & Corporate Affairs

Attachment

cc: Rear Admiral Craig E. Bone, Director of Port Security, US Coast Guard
Secretary Michael Chertoff, US Department of Homeland Security



1220 L Street, Northwest
Washington, DC 20005-4070
(202) 682-8482
(202) 682-8051 fax
gordonc@apl.org

Cindy L. Gordon
Security Team Leader

May 17, 2005

Mr. John Schwartz
Asst. Director, TWIC Program
Transportation Security Administration
TSA Headquarters – East Building (E8-210S)
8th Floor (TSA-19)
601 South 12th Street
Arlington, VA 22202-4220

CDR Cyndi Stowe
USCG
Chief, Vessel & Facility Security Division
United States Coast Guard
2100 Second Street, S.W.
Room 2408
Washington, DC 20593-0001

RE: MTSA TWIC Rulemaking

Dear Mr. Schwartz and CDR Stowe:

The American Petroleum Institute (API) is a national trade association with over 400 members engaged in all facets of the oil and natural gas industry, including exploration and production, transportation (marine, rail/truck and pipeline), marketing, and refining. API has been actively engaged in critical infrastructure initiatives with the U.S. Department of Homeland Security, the U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), the Department of Energy and other federal agencies.

API worked closely with the U.S. Coast Guard during the development and implementation of the Maritime Transportation Security Act (MTSA) and RADM Hereth thanked API and member companies for our cooperation. API's active understanding of the MTSA regulations resulted in minimal security plan deficiencies. We now understand that TSA and the USCG will propose a joint rulemaking this summer, which would require all workers needing unescorted access to secure areas in MTSA facilities to obtain a universal identification card (TWIC).

We appreciated the time Mr. Schwartz and LTjg. Nanine Nymen dedicated to API's Security Committee on April 28th. Based on that discussion, we would like to reiterate a significant employment concern we have in situations where an applicant is denied a TWIC.

We are concerned that employers will be put in an untenable position if TSA/USCG denies a TWIC card to an employee but does not advise the employer of the reason for the denial. Denial of the TWIC card places the employer on notice that the government has determined that the employee is a probable security risk or is otherwise unfit to work unescorted in a secure area. The Occupational Safety and Health Act states that the workplace should be safe and secure from recognized hazards. 29 U.S.C. § 654(a)(1). Denial of the TWIC to a current employee without notification of the reason for denial to the employer could compromise the safety of the workplace, since the employer would not know the basis for the denial and whether to remove the "TWIC denied" employee from the site or specific activities.

An employer could also be subject to negligent hiring/retention lawsuits if they take no action after becoming aware of such a potential concern. An employer cannot make an intelligent, informed decision as to the potential threat the involved employee may pose to the facility or other employees, if the regulations do not contain a mechanism to provide employers with sufficient information to understand and resolve these issues. Reassigning the employee to an area that does not require a TWIC card would not resolve the issue because the company would still face the same unanswered general security issues, and termination may be the only alternative left to the employer.

This concern is not new to TSA. Stakeholders raised similar concerns during development of the Patriot Act regulations. To alleviate this concern, API requests that the TSA/USCG include a waiver/release provision in the proposal, which would allow a "TWIC" applicant to request that TSA/USCG release the reason for the denial to an employer. Employers should be allowed to make the execution of such a release a condition of employment. We believe this would allow employees that are not a true security threat to be transferred to a different area in the company to keep their jobs, eliminate the mystery around the reasons for the denial, and ensure the employers can make informed and above all, safe decisions for all workers and neighboring communities.

Please feel free to contact me to discuss this concern further.

Sincerely,

A handwritten signature in black ink that reads "Cindy Gordon". The signature is written in a cursive, flowing style.

Cindy Gordon