

**LEGISLATIVE & PUBLIC POLICY ADVISORY**  
**Global Security & Enforcement**

June 22, 2006

**Proposed Rule on Transportation Worker Identification  
Credential (TWIC) Program**

On May 22, 2006, the Department of Homeland Security (“DHS”), with participation from the Transportation Security Administration (“TSA”) and the U.S. Coast Guard, published its proposed joint rulemakings for implementation of the Transportation Worker Identification Credential (“TWIC”) program. The impetus for this initiative stems from specific requirements outlined in the Maritime Transportation Security Act of 2002 (“MTSA”). Congressional focus on this program has also increased since the proposed DP World acquisition of Peninsular & Oriental Steam Navigation Company (“P&O”) port leases became public earlier this year and DP World, after intense congressional and media criticism, decided to divest itself of those assets.<sup>1</sup>

The joint TSA and U.S. Coast Guard rule generally proposes that all persons who require unescorted access to secure areas of a regulated U.S. port, facility or vessel, including “mariners holding an active License, Merchant Mariner Document or Certificate of Registry or STCW endorsement issued by the Coast Guard” must carry a TWIC card.<sup>2</sup> A TWIC card is defined as a “[f]ederally-issued biometric credential that TSA issues to an individual who has successfully completed a security threat assessment.”<sup>3</sup>

In a separate rulemaking the U.S. Coast Guard proposes to amend present maritime security regulations to incorporate the requirements of the TWIC program, in an effort to establish a single standard in the credentialing of maritime transportation workers.

This advisory briefly summarizes the proposed TSA and U.S. Coast Guard joint rulemakings and provides a general outline of the TWIC program and its requirements. Overall, the implementation of this program will affect the operational management of the transportation industry.

<sup>1</sup> See John Frittelli & Jennifer E. Lake, *Terminal Operators and Their Role in U.S. Port and Maritime Security* (CRS Report for Congress 2006) at <http://www.opencrs.com/getfile.php?rid=47451>.

<sup>2</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,449 (May 22, 2006) (to be codified at 46 C.F.R. pt. 15.415).

<sup>3</sup> Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,422 (May 22, 2006) (to be codified at 49 C.F.R. pt. 1570).

## Background and Purpose

The navigable waters of the United States encompass over 300 sea and river ports.<sup>4</sup> The United States specifically depends upon the operation of 17 U.S. ports for national security purposes.<sup>5</sup> To sustain the viability of the maritime industry, the United States employs several hundred thousand nationals and foreign nationals annually.<sup>6</sup> Authentication and verification of the identity of maritime transportation workers is crucial to preventing terrorists from gaining access to critical aspects of the maritime transportation system.<sup>7</sup>

In the wake of September 11th, a consensus developed that U.S. ports, facilities and vessels are vulnerable and susceptible to future threats upon the United States. Credentials used in the maritime transportation industry are vulnerable to fraud and tampering. TSA developed TWIC to strengthen the inherent weaknesses in the credentialing systems of the present transportation industry.

TSA and the U.S. Coast Guard have proposed the TWIC program pursuant to the Homeland Security Presidential Directive 12 (“HSPD 12”) and the MTSA. HSPD 12 mandates federal agencies to implement a secure identification credential scheme for both federal employees and contractors. TWIC satisfies the domestic credentialing requirements of MTSA. The MTSA specifically sets forth the legal authority permitting TSA to subject credentialed merchant mariners and workers, who have access to secured areas of U.S ports, facilities and vessels, to a security threat assessment and the issuance of a biometric credential or TWIC card.<sup>8</sup> A secured area for the purposes of these rules is defined as “the area on a vessel, maritime facility, or outer continental shelf facility where security measures have been implemented in a security plan approved by the Coast Guard.”<sup>9</sup>

## What information will a TWIC card reflect?

A TWIC card will contain the applicant’s digital photo, fingerprints, name, expiration date, PIN and credential number identification. The card, once issued to an applicant, will be valid for five years. The information stored on the card is both secured and encrypted, hence protected from tampering and fraud.

<sup>4</sup> See John Frittelli, *Port and Maritime Security: Background and Issues for Congress* (CRS Report for Congress 2005), available at <http://fas.org/sgp/crs/homesecc/RL31733.pdf>.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> See William H. Robinson, Jennifer E. Lake & Lisa M. Seghetti, *Border and Transportation Security: Possible New Directions and Policy Options* (CRS Report for Congress 2005), available at <http://www.opencrs.com/getfile.php?rid=47451>.

<sup>8</sup> Pub. L. No. 107-295, 116 Stat. 2064 (2002).

<sup>9</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,422 (May 22, 2006) (to be codified at 49 C.F.R. pt. 1570) (“For the purposes of TWIC, the secure area is the area in which a TWIC is required unless under escort”).

## The Transportation Port Worker Interim Screening Program

TSA has instituted an interim program that implements one aspect of the TWIC program. The Transportation Port Worker Interim Screening Program, which is in place until the joint rules are approved, requires that general facility operators and “employees and long-term contractors requiring access to [maritime] facilities,” submit identifying information that is subjected to a review by TSA and the Terrorist Screening Center.<sup>10</sup> Applicants who have successfully passed the screening are permitted to use a TSA approved form of credential,<sup>11</sup> pending the issuance of a TWIC card, to gain access into secure areas.

### Overview of TWIC

TSA estimates that the proposed regulations will directly impact over 750,000 people who work within the maritime transportation industry. This estimate, however, does not include commercial drivers who transport hazardous materials and who are already subject to a similar security threat assessment. Although the proposed joint rulemakings “primarily impact merchant mariners and port workers,” individuals who work in other sectors of transportation and require unescorted access to secured areas of vessels and facilities may be affected.<sup>12</sup> Those who will be subject primarily to the proposed rules include: “Cruise Workers (land-based only), Longshoremen, Merchant Mariner document of license holders, Off-shore Liquid Bulk Workers (i.e., MODU’s), Rail Workers, Shipyard Workers, Site Management/administration workers, Truck Drivers, Vessel Operation/Port Support Workers, Contractors/others.”<sup>13</sup>

The emphasis of the proposed rulemakings focus separately on the implementation of the TWIC program from an owner and operator perspective, and then outline the procedure for obtaining a TWIC. TSA will be largely responsible for the implementation and maintenance of the TWIC program. TSA will supervise the enrollment process, conduct the security threat assessment and approve applicants for the issuance of a TWIC, and oversee the appeals process for those denied a credential. The U.S. Coast Guard seeks to amend its present regulations enforcing vessel and facility security to require the use of TWIC to support pre-existing security access control systems.

---

<sup>10</sup> See *Transportation Port Worker Interim Screening Program* (U.S. Coast Guard Transportation Administration 2006), available at <http://www.uscg.mil/hq/g-m/mp/pdf/Part125GuidanceFinal.pdf>.

<sup>11</sup> See *id.* (“Credentials that can be used by individuals who have undergone the background check may include a state-issued driver’s license, facility-issued identification, a union or trade association-issued identification credential, merchant mariner’s document, Armed Forces Identification Card, credentials issued by Federal law enforcement or intelligence agencies, identification credentials issued to police and fireman, or any identification credential approved by the Commandant”).

<sup>12</sup> See *Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector*, 71 Fed. Reg. 29,405 (May 22, 2006) (stating that “for instance, many ports include railroad operations. Rail employees may be required to obtain a TWIC depending on whether the railroad operations are situated in the secure areas. Commercial truck drivers delivering or retrieving goods at the port typically have unescorted access to secure areas and so they would be required to have a TWIC”).

<sup>13</sup> See *Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector*, 71 Fed. Reg. 29,427 (May 22, 2006).

In general the proposed joint rules as applied to:

- **Applicants:** require workers in the maritime transportation industry, who hold a valid License, Merchant Mariner Document, or Certificate of Registry and require unescorted access to secure areas at maritime facilities or on a vessel, to undergo a TSA security threat assessment and carry a TWIC card;
- **Maritime regulations:** amend present Maritime regulations outlined in 33 C.F.R. parts 101-106 to require vessel and facility security to implement TWIC as an additional access control measure to enhance existing internal security standards;<sup>14</sup>
- **Consolidating Transportation Worker Identification Credentials:** consolidate existing licensing and documentation requirements for transportation workers and adopt a standard identification or background check requirement scheme; and
- **Service fees:** impose a service fee charge for the TWIC card.

Although not extensively addressed in the joint rulemakings at present, TSA may potentially expand the scope of the proposed TWIC program in the future to encompass all individuals who work in the transportation industry. Under the proposed rulings, however, foreign vessels are exempt from meeting the TWIC requirements.

The proposed regulations will place significant requirements upon employers who are tasked with the role of ensuring compliance. Employers are responsible for implementing the system, maintaining a backup security system in case there is a failure in the biometric access control points, sponsoring employees, notifying employees of the enrollment process and ensuring that TWICs are valid.

Owners must install TWIC readers, which will require positive photo and fingerprint identifications from employees seeking unescorted access to secure areas before gaining entry. The TWIC reader will only grant access to a cardholder after verifying a 1-to-1 match of the information provided by the cardholder to the biometric data stored in the system. The U.S. Coast Guard, under the proposed rules, will require owners and operators to draft and submit a TWIC Addendum to their security plans. A TWIC card, however, will not grant immediate access to secured areas. Access will still be subject to the discretion of the employer.

## TWIC Application Process

The application process may present the greatest challenge to the implementation of the TWIC program. TSA and the U.S. Coast Guard foresee the implementation of the TWIC program taking place over a period of 18 months.

---

<sup>14</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,409 (May 22, 2006) (to be codified at 33 C.F.R. 104.200, 104.210, 104.215, 104.220 and 104.225) (specifically proposing to “require that all individuals with security duties, including the company security officer (CSO), acquire and maintain a TWIC”).

TSA has identified 125 locations where enrollment centers can be established. Enrollment centers will begin accepting applicants at the end of 2006. TSA, however, does not anticipate completing the initial enrollment process until the end of 2008.

An applicant will be required to visit an enrollment site and submit biographical information that TSA will use for a security threat assessment. The applicant must bring a valid photo-ID and provide all ten fingerprints. Only after the applicant passes the TSA security assessment will TSA issue him/her a TWIC card.

The security threat assessment includes a review of the applicant's criminal background, immigration status, if applicable, and existing intelligence records to determine if the applicant poses a threat. This security threat assessment uses the same standards applied for commercial motor vehicle drivers licensed to transport hazardous materials within the United States. The proposed rulemakings publish a list of disqualifiable offenses. Included among those offenses, which can disqualify an applicant from receiving a TWIC, is a felony conviction within the last seven years.

## Fiscal Considerations

TSA estimates that it will cost approximately \$36.1 million to support the TWIC program for a period of five years. TSA proposes a total fee charge of between \$95 and \$149 for TWIC applicants.<sup>15</sup> This cost will subsidize the associated costs related to implementing the joint rulemakings, which include threat assessment, credentialing and other program management and oversight requirements. The proposed rulemakings, however, do not address whether the agency or the employer will bear the burden of the costs for equipment and computer programming to maintain the identification system.

## Issues that Companies Must Consider Under the Proposed Rules

**Enforcement:** Once approved the implementation of the rules will be mandatory, and companies can anticipate enforcement of these rules by TSA and/or the Coast Guard.

**Immigrant Employees:** TWIC applicants must be U.S. citizens or legal permanent residents. Because under the proposed rulemakings employees on foreign vessels are not required to implement TWIC, companies must take into consideration the requirements that workers from foreign ships, who wish to work upon a U.S. flagged vessel, would need to meet to receive escorted access<sup>16</sup> into secured areas.

---

<sup>15</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,428 (May 22, 2006) (estimating the following associated costs to include: "(1) information collection/credential issuance: \$45-65; (2) threat assessment/credential production: \$50-\$62; (3) credential replacement: \$36; (4) FBI: \$22").

<sup>16</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,437 (May 22, 2006) (to be codified at 33 C.F.R. pt. 101.105) (defining escorting as "ensuring that the escorted individual is continuously accompanied or monitored while within a secure areas in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted").

**Disqualified Applicants:** The offenses that can disqualify an applicant from receiving a TWIC card are very broad and in some instances unrelated to the specific MTSA security access concerns. Some disqualifying offenses and conditions included under the proposed rulemakings are:

- Arson
- A crime involving a transportation security incident as defined in 46 U.S.C. § 70101, which includes but is not limited to, the loss of life, environmental damage, transportation disruption or economic disruption
- Drug-related crimes
- Murder
- Violation of the Racketeer Influenced Corrupt Organizations (“RICO”) Act
- Robbery
- Lack of mental capacity

In general applicants who have been convicted within the past seven years will be disqualified. TSA, in some cases, may waive disqualifications and provide an appeal for applicants denied a TWIC card.

**Compliance Fees:** The projected costs of purchasing and installing a TWIC reader, depending on the size of the vessel or facility, will range from \$9,000-\$11,000.<sup>17</sup> However, it is unclear whether this cost includes the necessity of large vessels and facilities to purchase multiple TWIC readers. Further, imposing this burden upon owners/operators to have TWIC readers that comply with TSA standards goes beyond the intent of the MTSA, which only requires TWICs, but not TWIC readers.

**Record requirement:** The proposed rulemakings impose a strict two-year record requirement for vessels and facilities. Records must reflect TWIC access or the identity of the escort in cases of non-TWIC holders’ access.

**Knowledge requirement:** Under the proposed rulemakings an owner/operator must “ensure that someone on the vessel know[s] who is on the vessel at all times.”<sup>18</sup> In addition, the rules do not include a formal training requirement, and thus the burden is upon the owner/operator and those with security duties to become intimately familiar with the TWIC credentialing technologies, reader system and access control points.

---

<sup>17</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,435 (May 22, 2006).

<sup>18</sup> See Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector, 71 Fed. Reg. 29,409 (May 22, 2006) (to be codified at 33 C.F.R. 104. 200, 104.210, 104.215, 104.220 and 104.225).

## Conclusion

Although it remains unclear precisely what immediate and long-term logistical and operational impact the TWIC program will have on the maritime transportation industry, the program will cost companies money to comply with the new requirements. Ultimately, the program is likely to be expanded to other transportation workers, not just those in the maritime transportation industry. If a company has concerns about the proposed rule, it should participate in the public comment period and raise objections now before the rule is implemented.

Companies affected by this proposed rule will be responsible for ensuring that they are fully compliant with the new requirements. Depending upon the circumstances involved, if an affected company fails to comply, it risks exposure to civil and criminal liability. In light of the emphasis being placed on homeland, border, transportation and port security by the U.S. government and the potential implications for transportation companies, it is essential that companies take proactive and prompt steps to satisfy the requirements of the rule once it is promulgated.

**The public will have until July 6, 2006, to comment on the proposed rule.**

This *Legislative & Public Policy Advisory: Global Security & Enforcement* is published by Alston & Bird ([www.alston.com](http://www.alston.com)) to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. The material may also be considered advertising under the applicable court rules. If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Thomas M. Boyd  
202-756-3372  
[tom.boyd@alston.com](mailto:tom.boyd@alston.com)

Eileen M. G. Scofield  
404-881-7375  
[eileen.scofield@alston.com](mailto:eileen.scofield@alston.com)

Kipp A. Coddington  
202-756-3408  
[kipp.coddington@alston.com](mailto:kipp.coddington@alston.com)

Jason M. Waite  
202-756-3455  
[jason.waite@alston.com](mailto:jason.waite@alston.com)

Thomas E. Crocker  
202-756-3318  
[thomas.crocker@alston.com](mailto:thomas.crocker@alston.com)

Kenneth G. Weigel  
202-756-3431  
[ken.weigel@alston.com](mailto:ken.weigel@alston.com)

Jonathan M. Fee  
202-756-3387  
[jon.fee@alston.com](mailto:jon.fee@alston.com)

Joe D. Whitley  
202-756-3189  
[joe.whitley@alston.com](mailto:joe.whitley@alston.com)

George A. Koenig  
202-756-3469  
[george.koenig@alston.com](mailto:george.koenig@alston.com)

Jonathan M. Winer  
202-756-3342  
[jonathan.winer@alston.com](mailto:jonathan.winer@alston.com)

*If you would like to receive future Legislative & Public Policy Advisories electronically, please forward your contact information including e-mail address to [legislative.advisory@alston.com](mailto:legislative.advisory@alston.com). Be sure to put "subscribe" in the subject line.*

ALSTON+BIRD<sup>LLP</sup>

[www.alston.com](http://www.alston.com)

#### ATLANTA

One Atlantic Center  
1201 West Peachtree Street  
Atlanta, GA 30309-3424  
404-881-7000

#### CHARLOTTE

Bank of America Plaza  
101 South Tryon Street  
Suite 4000  
Charlotte, NC 28280-4000  
704-444-1000

#### NEW YORK

90 Park Avenue  
New York, NY 10016-1387  
212-210-9400

#### RESEARCH TRIANGLE

3201 Beechleaf Court  
Suite 600  
Raleigh, NC 27604-1062  
919-862-2200

#### WASHINGTON, DC

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404  
202-756-3300

[www.alston.com](http://www.alston.com)