June 20, 2013

Via Electronic Submission

U.S. Coast Guard
Department of Homeland Security
Washington, DC 20528-8610

Re: Transportation Worker Identification Credential Reader;
Notice of Proposed Rulemaking – RIN 1625-AB21

Introduction

The American Trucking Associations, Inc. (ATA)\(^1\) files these comments in response to the U.S. Coast Guard, U.S. Department of Homeland Security, Notice of Proposed Rulemaking (NPRM) in the Federal Register on March 21, 2013, detailing proposed regulations mandating the installation of TWIC readers at the entrance of secure areas of maritime facilities. This long awaited proposed rule implements legislative mandates included in the Maritime Transportation Security Act (MTSA) of 2004 and in the SAFE PORT Act of 2006. Specifically, the NPRM proposes to have installed readers at certain MTSA-regulated facilities electronically match the biometric and biographic information encoded in the TWIC with a biometric provided by the holder of the credential seeking unescorted access to the secure areas.

As a national trade association representing the interests of the trucking industry, ATA supports efforts and programs that improve the safety and security of our Nation’s critical infrastructure while also ensuring that such measures do not have an unnecessarily burdensome or negative impact on motor carrier operations. Due to the nature of such operations, trucks are ubiquitous throughout the entire transportation system, picking up and delivering commodities to and from air, rail, manufacturing, retail and maritime facilities, and across state and international borders. In essence, the trucking industry plays an essential role in transporting cargo moving through both domestic and international supply chains.

\(^1\) ATA is a united federation of motor carriers, state trucking associations, and national trucking conferences created to promote and protect the interests of the trucking industry. Its membership includes more than 2,000 trucking companies and industry suppliers of equipment and services. Directly and through its affiliated organizations, ATA encompasses over 34,000 companies and every type and class of motor carrier operation.
According to TSA data, nearly 450,000 drayage and regular truck drivers are in possession of TWICs, a number that far surpasses the original estimate of 110,000 port truck drivers provided by TSA and USCG in their joint NPRM to implement the TWIC in the maritime sector.\(^2\) It is also important to note that commercial drivers are the single largest defined occupational category possessing TWIC, including both drayage and long-haul operations. Thus, ATA is following the implementation of the TWIC program with great interest, including the implementation of TWIC readers proposed in this notice.

**Comments to Specific Requirements and Issues**

**Risk-based approach for requiring readers at certain facilities:** The USCG is proposing to rank ports into three levels of risk: A, B and C. Only ports ranked in the “A” risk category – the USCG estimates there are 532 such venues representing less than 5 percent of the MTSA regulated facilities – would be required to install readers at access points to each secure area. USCG has determined that these facilities face a greater risk for a Transportation Security Incident (TSI) and represent a larger economic and national security impact. The USCG proposes to mandate the installation of TWIC readers in “A” facilities within two years from the issuance of the Final Rule. During this two year period facilities should install the readers and also provide the necessary training and testing to ensure that the reader users are able to operate the equipment correctly.

Facilities ranked as “B” and “C” would not be required to install readers but would be required to continue checking TWICs visually. USCG emphasizes that it has the authority to amend this risk-based approach to expand the use of the readers at B and C facilities if deemed necessary.

Although ATA and its members have long supported the use of “risk-based” approaches by government agencies in developing security regulations that impact trucking operations, for example, in the transportation of hazardous materials, we are concerned that a tiered implementation of TWIC readers could pose potential challenges.

Although a risk-based approach is an important consideration for implementing any security regulation, a lack of uniformity in implementing the TWIC readers throughout all MTSA-regulated facilities could result in a confusing panoply of entry verification and inspection processes and requirements established by “B” and “C” facilities, especially for commercial drivers who visit various ports during their itinerant operations. Establishing a uniform access process is important to avoid confusion and to avoid any potential delays resulting from uncertainty or unfamiliarity with site-specific procedures. Furthermore, installing TWIC readers throughout the entire MTSA-regulated spectrum of facilities would also eliminate the potential for subjectivity by personnel visually inspecting and handling TWICs at entry points.

\(^2\) 71 Federal Register at 29427 (May 22, 2006)
The protection of our national transportation infrastructure is of vital interest to motor carrier operations. This proposal would weaken the overall security goal of the TWIC smart card if the vast majority of MTSA-regulated facilities lack the electronic card verification to authenticate the validity of the card as well as the identity and status of the cardholder. Trucking companies and commercial drivers have invested heavily in applying and paying for a high-tech and expensive credential, at roughly $130 per TWIC, explicitly designed to be operated in conjunction with card readers. If such readers will not be available at over 95 percent of MTSA-regulated facilities, then the TWIC program serves little purpose in protecting our critical maritime transportation infrastructure as original intended.

Furthermore, the USCG states in its NPRM that it reserves the right to implement readers at other locations if needed: “Proposing TWIC reader requirements for Risk Group A only in this NPRM is indicative of our desire to minimize highest risks first, but should not be read to foreclose revised TWIC reader requirements in the future.” If the USCG determines, either after a TSI or due to an increased MARSEC threat level, to require all MTSA-regulated facilities to install readers, it could take a long time for non-compliant impacted facilities to acquire the necessary readers.

ATA requests that the USCG require “A” and “B” risk category facilities to have permanent readers installed, and that “C” category facilities maintain a certain number of mobile readers if needed. TWIC readers are necessary to ensure operational uniformity for entry processes, as well as for credential, identity, and status verification through the Cancelled Card List (CCL).

Recordkeeping requirement of entries: The USCG proposes to require owners and operators of facilities with TWIC readers to maintain records on each individual granted access to MTSA-regulated secure areas, including commercial drivers. The NPRM states that each individual’s transaction information should be kept for at least two years.

ATA is concerned about safeguards regarding how commercial drivers’ data and information will be stored and secured by the owners and operators of the facilities collecting such information. In the NPRM, USCG does not provide detailed information as to how such data should be stored and maintained, for two years, should the agency seek access to such information.

ATA requests that the USCG provide specific information regarding what requirements are being established for owners and operators to secure the privacy of data and information provided by TWIC cardholders every time they access a regulated facility.

Alternative entry procedures when readers malfunction or damaged/lost TWIC: If and when TWIC readers are damaged or not working properly at a facility, the USCG proposes to allow owners or operators of such a facility to revert to visual inspections for up to seven days if certain conditions are met. In addition, the Captain of the Port (COPT) has the discretion to extend the period beyond seven days if necessary.
In addition, TWIC holders who have either lost their TWIC or had it stolen will continue to have access to secure areas for seven consecutive days as long as: the individual has been known to have a TWIC and has reported it lost or stolen, the individual presents another ID that meets certain requirements (contain biographical information, photo, be laminated and be government issued or by an approved entity), and no suspicious circumstances surround the loss or theft. In this case the COPT has authority to extend the period to 30 days.

ATA supports these alternative entry policies for transportation workers.

Training and potential delays impacting throughput at maritime facilities: The USCG describes in the NPRM the potential for confusion by TWIC holders who have to interact with diverse types of readers at different facilities. The USCG states that “switching between different TWIC reader modes of operation negatively impacted the efficiency of TWIC reader use by complicating the learning process for TWIC-holders.” The USCG adds that TWIC-holders “were confused by the different procedural requirements for the different TWIC reader modes of operation, regardless of attempts to inform TWIC-holders in advance of mode changes.” Specifically, the NPRM describes how “truck drivers visiting several facilities encountered TWIC readers that were sometimes placed at awkward heights or distances making the readers difficult to reach.”

ATA agrees that it is important to have a “consistent user experience”. The USCG should mandate a uniform system and processes for TWIC readers to avoid potential access delays due to a multiplicity of reader systems or improper installation from port to port. The COPT has authority to “suspend” the TWIC reader requirements if it determines they are causing delays and "excessive vehicle buildup" or other unintended consequences.

No use of PIN: ATA has received feedback from motor carrier members and their drivers that a PIN requirement could have a negative operational impact at secure area entry points for commercial drivers, which would likely impact equipment throughput into the facility resulting in significant delays. These delays are likely to worsen if drivers have problems typing PIN numbers into reader keypads. Such problems could be further exacerbated during bad weather conditions or if cardholders have trouble remembering or finding their PINs.

ATA agrees and supports the USCG’s decision not to require the use of the Personal Identification Number (PIN) associated with each TWIC when transportation workers enter the secure areas of MTSA-regulated facilities.

Preemption: ATA strongly supports the NPRM’s pre-emption principles statement affirming that the TWIC Reader Requirements foreclose States and local governments from implementing similar or additional requirements in this area.
Attack Scenarios Evaluated: The USCG evaluated three scenarios that the agency believes could be mitigated through the use of TWIC readers and the enhanced security features provided by the equipment. These scenarios included in the NPRM are: 1. Truck bomb, 2. Terrorist Assault Team, and 3. Passenger/Passerby Explosives/Improvised Explosive Device.

Scenario 1 is described as follows: “Armed terrorists use a truck loaded with explosives to attack the target focal point. The terrorists will attempt to overcome guards and barriers if they encountered them.” In this scenario we infer that the driver, alone or accompanied, is a potential terrorist who purportedly loaded the truck with explosives and will try to gain entry into the secure area of a port. Terrorists are unlikely to try such an attack if their intent is to blow up the container within the port’s secure areas to achieve maximum impact. This simplified Truck Bomb scenario described in the NPRM’s Regulatory Analyses section does not apply or represent a realistic scenario with which to provide consequence data in analyzing the benefits from implementing the TWIC reader.

A more probable scenario would likely involve loading explosives into a container concealed as a load of general cargo bound for export on a Bill of Lading (BOL). Such a load could form part of a Less-than Container Load (LCL) shipment, resulting in the driver having little or no knowledge of the multiple contents in the container. The container could be tracked or followed until it reaches a desired location for detonation. This scenario corroborates the USCG’s statement in the NPRM that “the use of TWIC readers, or other access control features, would not mitigate the threat associated with the contents of a container.”

Conclusion

The TWIC program provides a robust STA and credentialing processes that can be expanded to satisfy compliance with multiple regulatory and programmatic security requirements including securing maritime facilities. Unfortunately, TSA and USCG have taken far too long to develop a NPRM requiring the installation of TWIC readers at MTSA-regulated facilities while cardholders have been paying a high fee to purchase the TWIC without the companion reader technology necessary to realize the full potential of the credential. So far the TWIC has functioned, as is commonly termed within the transportation sector, as an expensive “flash-pass.”

The TWIC reader NPRM is critical in fulfilling a key goal of the overall TWIC program to allow for the verification and authentication of the credential, as well as matching the credential to the cardholder’s identity. ATA supports the implementation of the TWIC readers in order to not only improve security, but to also improve throughput at maritime facilities for commercial vehicles. To summarize, the following issues are recommendations and concerns that USCG and TSA should address to ensure a uniform and improved implementation of the TWIC reader rule:

- ATA supports a risk-based approach in implementing security regulations, but the use of TWIC readers should be expanded beyond Group A, to include
Group B or all regulated facilities in some form, rather than continuing to utilize expensive TWIC smart cards as “flash-passes” for visuals inspections;

- TSA and USCG must develop specific recordkeeping requirements for information collected and stored by MTSA-regulated facilities from TWIC cardholders to protect the privacy and security of such data;

- Establish uniform TWIC reader standards at all facilities and establish a true “consistent user experience” to minimize any potential problems with variances in equipment, additional training needs, and overall user difficulties.

ATA supports the following proposals within the NPRM:

- Establishing alternative entry procedures when readers malfunction or when cards are lost or damaged, and providing the COPT greater flexibility in extending such periods if necessary;

- Not requiring the use of the TWIC PIN at readers when entering a secure area of a facility, which would significantly increase processing times;

- Establishing preemption to avoid potential duplicative processes by State and local authorities.

It is also important to note the ATA and the motor carrier industry continue to have grave concerns with particular issues related to the TWIC, including:

- The high cost of the TWIC at $129.50;

- The long processing and wait-times the TWIC application requires for providing biographic and biometric data, as well as the required time off work;

- The need to coordinate the portability and acceptability of the TWIC for complying with other federal programs requiring STA or PIV standards;

- The need to increase the number of STA enrollment facilities nationwide.

Thank you for the opportunity to provide our input and comments and we look forward to working with DHS, USCG and TSA in strengthening our country’s security posture while also improving our commercial and economic wellbeing.

Should you have any questions or seek further input from ATA on the information provided above, please contact me at (703) 838-7950.

Respectfully submitted,

[Signature]

Martin Rojas
Vice President, Security & Operations