Response to Written Question Submitted by Hon. John Thune to Chris Spear

Question. Mr. Spears, there has been a lot of discussion of the TWIC program. I hear the program has progressed, but I am interested in your thoughts. Is the TWIC program providing the verifications you need and how would you like to see the program changed?

Answer. ATA continues to support the concept of a single, federally-issued credential for transportation workers to satisfy multiple security threat assessment (STA) requirements. The TWIC is a robust, standardized credential that, when paired with appropriate card readers, has the potential to serve as a valuable and effective tool to enhance the security of our ports and other critical infrastructure. Unfortunately, drivers with TWIC cards are still subjected to multiple, identical STAs to obtain separate credentials in order to access other highly secure facilities and haul hazardous materials. This has resulted in the costly and inefficient environment that motor carriers and drivers operate in today. So long as there is no one single, universally-accepted credential, the full potential of the TWIC cannot be realized.

Under the law, TSA may only perform STAs for a TWIC card on workers “engaged in the field of transportation”. Recently, TSA amended its legal interpretation of “field of transportation” to cover “any individual, activity, entity, facility, owner, or operator that is subject to regulation by TSA, Department of Transportation, or the US Coast Guard , and individuals applying for trusted traveler programs.”[1] ATA supports this new interpretation which will greatly expand the number of individuals in the coming years who apply and pay for a STA and TWIC card. As more TWIC cards are issued, the establishment of the TWIC as the single, national, uniform credential becomes more critical in order to reduce inefficiencies and lift the burden of undergoing duplicative background checks and obtaining multiple credentials.

[1] 81 Federal Register No. 188; 66671-66672; https://www.gpo.gov/fdsys/pkg/FR-2016-09-28/pdf/2016-23370.pdf

Response to Written Questions Submitted by Hon. Deb Fischer to Chris Spear

Question 1. Mr. Spear, what type of policies would a Security Threat Assessment include, in your opinion? In addition to a single credentialing system, what other policies would streamline the security process without degrading our security?

Answer. Currently, the Security Threat Assessment associated with the TWIC and HME requires a FBI criminal history records check, a check against the Terrorist Screening Database, proof of citizenship or immigration status, and proof of identity. As far as the industry is concerned, these checks are sufficient in determining whether an individual poses a threat to national security.

Although a single credentialing process would maximize efficiency while maintaining security, there are other ways to streamline the process. The first would be better communication. The Department of Homeland Security was created by the Homeland Security Act of 2002. This act brought 22 federal agencies underneath this new cabinet level department. We believe the department has worked through a number of early concerns, but the industry still faces the situation of being faced with a number of agencies regulating security.

If a driver is screened for a TWIC card, that screening should work for an HME. The background check information used for that screening should not be different, if that driver wanted to apply for TSA precheck, for personal travel. Should there be a reason that a TSA officer does not recognize that the TWIC can be used to board an airplane? The agencies should coordinate their efforts, to minimize overlap and reduce customer frustration. The ability to immediately verify an applicant has been cleared and does not pose a security risk to the Pipelines and Hazardous Materials Administration, should allow for an expedited clearance with the Federal Aviation Administration. Those databases should be able to communicate with one another.

Record keeping is another concern when it comes to streamlining the process. Every five years a new set of fingerprints must be taken to receive a TWIC. According to the Department of Homeland Security Privacy Impact Assessment for the Transportation Worker's Identification Credential[2], biometric records are retained on an individual while they remain an active TWIC card holder. Upon expiration of the TWIC, those records are destroyed. ATA believes that if that individual would like to continue to transport commodities to port facilities and renew their TWIC, the records should not be destroyed but be retained for the length of the renewal.

Question 2. You mentioned in your written testimony concerns about the GAO's recommendations for "alternative" credentialing methods, including the potential for a

[2] U.S. Department of Homeland Security. *Privacy Impact Assessment for the Transportation Workers Identification Credential Program,* Oct 5, 2007. Available at: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_twic09.pdf

decentralized system (whereby each entity has its own port security systems). Can you elaborate further on these concerns?

Answer. A decentralized approach would be disastrous from both an operational and a cost standpoint. Allowing states and localities or individual facilities throughout the country to establish their own STA requirements and issue separate credentials could create confusion regarding site-specific access requirements, especially for those transportation workers who operate at multiple Maritime Transportation Security Act (MTSA) regulated facilities. Furthermore, a decentralized approach would only add to the costs already imposed on motor carriers and drivers today. While establishing additional requirements and credentials for access may be a boon for cash-strapped states and localities, requiring a driver who holds a valid TWIC card to undergo duplicative STAs would waste government resources and create an increasingly burdensome and inefficient operating environment without enhancing security. For these reasons, ATA continues to support the "one credential or screening, many uses" policy that Congress envisioned when creating the TWIC nearly fifteen years ago.

Question 3. What are your thoughts on the United States Coast Guard's (USCG) August 2016 final rule that will require high-risk category facilities and a vessel to incorporate an electronic TWIC validation process, which includes a biometric check for high-risk category facilities and a vessel, prior to entry into a secured area?

Answer. In the final rule, the Coast Guard only requires ports designated as "Risk A" facilities to install TWIC readers at access points to secure areas. Facilities not designated as "Risk A" facilities are not required to install readers, but are required to continue visually inspecting TWICs. Although ATA and its members support the use of such risk-based approaches in developing security regulations, in this particular situation, we are concerned about the lack of uniformity in implementing TWIC readers throughout all MTSA-regulated facilities.

For one, the lack of a uniform access process across MTSA-regulated facilities could create delays resulting from uncertainty or unfamiliarity with site-specific entry verification and inspection processes, especially among commercial drivers who service multiple ports during their operations. Secondly, installing TWIC readers at additional MTSA-regulated facilities would eliminate the potential for subjectivity by personnel visually inspecting TWICs at entry points. Since readers to authenticate the card's validity, as well as the driver's identity and status, will not be available at over 95 percent of MTSA-regulated facilities, the overall security goal of the TWIC card is undermined. Finally, motor carriers and commercial drivers have invested heavily in applying and paying for what was promised to be a high-tech, secure credential designed to be operated in conjunction with electronic readers. In reality, however, what they have functionally paid for is an expensive "flash pass," since most facilities will not have readers installed to make use of the card's full potential.

ATA believes expanding the scope of the requirement to additional MTSA-regulated facilities will further our shared goal of protecting our nation's critical transportation infrastructure, reduce confusion at port secure entry points, and fulfill the promise of the TWIC card program.

Question 4. The August 2016 TWIC reader rule also states that, while not required, a maritime operator can utilize electronic TWIC inspection on a voluntary basis if they feel that this provides an additional level of security protection - and many have chosen to incorporate TWIC electronic readers into their USCG facility security plans. Are you seeing the biometric check being utilized beyond the category facilities that will be subject to USCG Final Rule?

Answer. It is encouraging to hear that some operators recognize the security and economic benefits that will come from installing TWIC readers and have chosen to do so voluntarily. However, without a requirement to install the TWIC readers, the vast majority of facilities will continue to rely on subjective visual inspections that will leave them vulnerable to security threats, undermining the goal of the TWIC program and endangering critical infrastructure.