

Before the

United States Senate

**Commerce, Science and Transportation
Subcommittee on Surface Transportation and
Merchant Marine Infrastructure, Safety and Security**

Statement of

American Trucking Associations, Inc.

For the Hearing on

Assessing the Security of our Critical Surface Transportation Infrastructure

December 7, 2016



**950 N. Glebe Road
Arlington, VA 22203
703-838-1996**

Introduction

Chairman Fischer, Ranking Member Booker and distinguished members of the subcommittee, thank you for the opportunity to testify today on “Assessing the Security of our Critical Surface Transportation Infrastructure.” My name is Chris Spear, and I am the President and CEO of the American Trucking Associations (ATA). Founded in 1933, ATA is the nation’s preeminent organization representing the interests of the U.S. trucking industry. Directly and through its affiliated organizations, ATA encompasses more than 30,000 companies and every type and class of motor carrier operation.

The trucking industry is an integral component of our nation's economy, transporting more than 80% of our nation’s freight and employing approximately 7 million workers in trucking-related jobs, including over 3.5 million commercial drivers¹. It is also important to note that the trucking industry is comprised primarily of small businesses, with 97.3% of trucking companies operating 20 trucks or less, and 90.8% operating six trucks or less.² Approximately 80% of all U.S. communities depend solely on trucks to deliver and supply their essential commodities³. Most importantly, the trucking industry now spends more than \$9.5 billion each year on safety enhancements to help ensure that drivers and passengers of all vehicles make it safely to their destination⁴.

ATA also places great emphasis on security. Our focus is on strengthening transportation security without undermining economic security. To do this, we must rationalize the various credential requirements commercial drivers use, whether it be one federally issued credential or a credential with a federal background check, such as a Hazardous Materials Endorsement (HME), to satisfy any federal regulation that requires a criminal history records check to operate in a facility or to conduct certain operations. Having drivers undergo multiple duplicative screenings undermines our nation’s economic security by posing a direct financial burden on drivers and motor carriers and further depleting scarce federal government resources. In short, this current and longstanding lack of coordination among federal agencies in harmonizing or coordinating screening requirements is not a viable operating environment for motor carriers and commercial drivers.

The Problem with Alternative Credentialing Approaches

Since the Maritime Transportation Security Act (MTSA) of 2002 (Sec 102 of PL 107-295) authorized the Transportation Worker Identification Card (TWIC), ATA has advocated a “one credential or screening, many uses” policy to balance the flow of commerce without compromising the security of our nation’s supply chain. ATA strongly believes that the TWIC can serve as a universal credentialing/background check as well as a physical access control security mechanism at regulated port facilities. If the goal for TWIC is to prevent acts of terror from occurring and to stop possible terrorists from obtaining access to secure areas of MTSA-

¹ American Trucking Associations, *American Trucking Trends 2016* (August 2016)

² American Trucking Associations, *American Trucking Trends 2016* (August 2016).

³ ATA staff, developed the 80% figure by using the Rand McNally Commercial & Marketing Guide (2001) numbers for rail service to communities and calculating the inverse, ultimately deriving the number of communities serviced by truck.

⁴ American Trucking Associations, (2016, June 26). *Trucking Industry Spends \$9.5 Billion In Safety Annually*. Retrieved from:

[http://www.trucking.org/ATA%20Docs/News%20and%20Information/Reports%20Trends%20and%20Statistics/06%2028%2016%20-%20Trucking%20Industry%20Invests%20\\$9%205%20Billion%20in%20Safety%20Annually.pdf](http://www.trucking.org/ATA%20Docs/News%20and%20Information/Reports%20Trends%20and%20Statistics/06%2028%2016%20-%20Trucking%20Industry%20Invests%20$9%205%20Billion%20in%20Safety%20Annually.pdf)

regulated facilities, one could argue that this objective is being met. Yet the timeline for achieving this goal is unsatisfactory at best. It has been 15 years since MTSA was enacted, 9 years since the TWIC final rule became effective, and still America has to wait two more years before TWIC readers are to be fully implemented. While one could argue that this is measurable progress, ATA believes that we can and must do better.

Redundancy of security threat assessments has still not been addressed. It has been 15 years since the tragic events of September 11th, yet commercial drivers are still required to get a background check for TWIC, HME and Free and Secure Trade (FAST), as well as different checks for airports. Imagine requiring two separate cards for getting to and from the House and Senate. That's just two locations. Now multiply that number by the thousands and we begin to understand what commercial drivers and carriers face every day. Currently, there are 2.1 million active TWIC cards out of more than 3.5 million issued⁵. When dealing with over 700,000 drivers⁶, that have acquired the TWIC since 2007; requiring access to thousands of sensitive sites throughout the nation, the numbers tell the story.

The Solution is TWIC

Adopting a “one credential or screening, many uses” policy would fix this problem. Absent this policy, ATA’s highest security priority will continue to be the multiplicity of background checks and their associated costs and burdens. Drivers must undergo these checks to perform their everyday work responsibilities, including transporting hazardous materials, delivering at maritime facilities, crossing international land borders and transporting air cargo. ATA has consistently supported a system and process that provides for a criminal history records check through national databases. Today’s threats aren’t against one or more states, but America itself. If we’re serious about protecting our homeland, then we must eliminate reactive behavior that results in redundant policies and practices. This is why ATA supports the TWIC as the potential single credential and Security Threat Assessment (STA) that, in turn, can demonstrate and provide compliance with multiple programs and regulations.

TSA has not yet provided for full recognition of one STA for compliance with another regulatory STA, for instance permitting TWIC holders seeking an HME to show their TWIC as proof of already having an equivalent STA. This is a policy that is supported statutorily by Section 1556 of the 9/11 Commission Act, whereas other federal agencies are accepting the TWIC for compliance with their credentialing requirements. For example, the Department of Defense (DOD) has established policy allowing commercial drivers transporting freight in and out of appropriate military facilities to use a TWIC in lieu of obtaining a DOD-issued Common Access Card (CAC). DOD acceptance of the TWIC for such purposes is recognition of the strength of the TWIC STA process and its compliance with federal Personal Identity Verification (PIV) standards used by millions of federal employees.

The Government Accountability Office (GAO) issued a report three years ago⁷ criticizing TSA’s planning shortfalls for implementing the TWIC reader pilot in a manner that did not yield usable information due to data-collection challenges. While ATA recognizes that TSA faced some technology challenges in collecting TWIC-reader functionality data, we would also point out that certain facilities using the TWIC readers successfully verified the credentials’ status, identifying and improving throughput for truck operations. Additional focus should be given to facilities that

⁵ Office of Inspector General; Department of Homeland Security (2016). *TWIC Background Checks are Not as Reliable as They Could Be* (OIG-16-128)

⁶ ATA staff was given this number by DHS, Office of Security Policy and Industry Management

⁷ Government Accounting Office (2013), *Transportation Worker Identification Credential: Card Reader Pilot Results Are Unreliable; Security Benefits Should Be Reassessed*, (GAO -13-695T)

have successfully implemented the TWIC readers, utilizing the “lessons-learned” and applying them to other facilities facing reader challenges.

ATA continues to voice its concern with GAO’s suggestion that Congress consider “alternative credentialing approaches, which might include a more decentralized approach for achieving TWIC program goals.”⁸ A decentralized approach is inherently flawed, will elevate security risks, inflict harm to our economy and further delay adoption of a “one credential or screening, multiple uses” policy. Specifically, a decentralized approach would result in an environment in which each state or location performs STAs and issues separate credentials for truck drivers to access maritime facilities throughout the country. Such a scenario would result in an increasingly burdensome, inefficient and ineffective system for transportation workers who work and operate at multiple MTSA-regulated facilities. In contrast, the TWIC serves as a robust, nationwide, uniform STA that can be utilized at multiple locations when matched with the appropriate readers. For GAO to legitimately stand by its recommendation for decentralization, it would first need to explain why DOD’s command and control administration of its CAC credential and the measurable benefits it provides its holders around the world should do the same. Such a suggestion would be baseless, just as it is for the TWIC credential. The TSA and Coast Guard need to focus their efforts on ensuring the successful deployment of TWIC readers nationwide rather than creating a vast assortment of individual systems, which, unfortunately our nation still has 16 years after TWIC was authorized by Congress.

ATA supports the implementation of the TWIC readers to improve security as well as throughput at maritime facilities for commercial vehicles. ATA asks Congress to remain vigilant during the implementation of the TWIC reader final rule; holding DHS accountable for ensuring that personnel working throughout our country’s critical transportation infrastructure have been properly screened and continue to be vetted through relevant databases. Moreover, when the credential is utilized with the appropriate readers, it can ensure the validity of the card, match the TWIC to the cardholder, and allow for improved throughput when entering secure areas requiring these systems.

Some TWIC Progress Being Made

Setting the ATA’s standing request for a “one credential or screening, many uses” policy aside, there are specific instances of progress with respect to TWIC that ATA can report to this subcommittee. In 2014 ATA submitted written testimony to the Senate Committee on Homeland Security and Governmental Affairs.⁹ At that time, we provided an update on several challenges and opportunities facing the full adoption of TWIC based on day-to-day experiences of the trucking industry, including:

- The excessively high cost of the TWIC;
- The extended time the application process requires of applicants, taking time off work twice; once to apply and provide the biometrics; and, a second visit to pick up the credential;

⁸ Federal Government Approaches to Issuing Biometric IDs: Hearing before the Subcommittee on Government Operations of the Committee of Oversight and Government Reform, House of Representatives, 113th Congress (2013) (Testimony of Stephen M. Lord)

⁹ Evaluating Port Security: Progress Made and Challenges Ahead: Hearing before the Committee on Homeland Security and Governmental Affairs, Senate (2014)

- The failure to expand TWIC's utilization to satisfy other federal STA regulatory requirements, including identical STA programs within the Transportation Security Administration (TSA);
- The past lack of TWIC enrollment facilities nationwide to facilitate the enrollment of transportation workers who live far from either coast; and,
- The failure to implement the TWIC rule with its essential counterpart reader rule, annulling the credential's technology benefits and serving only as an expensive "flash-pass."

Since citing these five concerns in 2014, ATA is pleased to report that it has witnessed moderate improvements. The cost of the TWIC just two years ago was \$129.50. It is now \$125.25 for new applicants; \$105.25 for new applicants with a valid HME; and, a replacement card is now \$60.00. That said, the combined costs for TWIC and HME screenings have well surpassed \$200 million, paid for entirely by the trucking industry as part of the overall cost to keep our nation safe.

While the TSA website still cites an extended wait time of 4 to 6 weeks for applications to process, TWIC applications are now reportedly being processed in as little as two weeks. Applicants also don't have to take as much time off to acquire their actual credential. In July of 2014, TSA allowed for the "one visit" program to go national. The second visit to pick up a TWIC from the enrollment center was no longer required. Applicants could now have their TWIC or replacement TWIC mailed to their home.

The failure to expand the utilization of TWIC has also improved since 2014, but unfortunately not by much. Drivers with TWIC cards are deemed to have met the requirements for the Personnel Surety Program (PSP) under Chemical Facility Anti-Terrorism Standards of 2014¹⁰ and have the ability to use the TWIC to enter covered facilities and installations.

The lack of enrollment centers has been addressed by the contractor as suggested in our 2014 testimony. Forty-one states now use the universal enrollment for TSA and the fingerprint locations can also be kiosks at state DMV's.

As for implementation of the reader rule, the U.S. Coast Guard put out this rule in August of this year and it is currently expected to go into effect August 23, 2018. The rule, however, uses a tier level system, where only the highest level are required to use the readers. If that occurs, many of ATA's members required to have TWIC may not have their card scanned.

ATA members, specifically drivers and carriers, will continue to serve on the front line where they experience the successes and shortfalls of TWIC. That being the case, ATA will continue to update Congress as well as provide comments to DHS and its agencies on these and any other challenges that may arise to help improve the TWIC program and balance the importance of transportation and economic security.

ATA supports the DHS serving as the primary authority in coordinating and managing security programs affecting the transportation sector. In that vein, harmonization and consolidation of motor carrier requirements pertaining to security background checks, security plans, security training and corporate security reviews is and remains an elevated industry priority. ATA also supports the Surface Transportation and Maritime Security Act (S. 3379) recently introduced by

¹⁰ Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014, Pub. L 113 -254. §2102, 128 Stat.2909 (2014)

the committee, which would take steps to reduce costly and unnecessary background check requirements on drivers, specifically by allowing TWIC holders to obtain their hazmat endorsement without the need for additional background checks. Such reforms will continue to improve the efficiency of goods movement without hindering our national security interests.

Cybersecurity

A secondary security priority for the ATA is the need to continue harmonizing any security requirement on carriers to harden their operations when transporting certain types of cargo or operating in environments that require a higher degree of security. Trucking is not exempt from the threats of cybersecurity. Our industry will continue to work with service providers as well as government agencies to improve our cybersecurity posture and make certain that our systems and protocols are never compromised.

The number of cyberattacks throughout the country continues to climb, compromising countless businesses and threatening consumer and personal privacy. Moving the majority of our nation's freight and adopting more technology that our industry requires to remain competitive and efficient makes trucking equally susceptible to cyber threats. Trucking companies have already been victims of "ransomware" (i.e. locked out of their servers with demands for money to resume access) and have had sensitive business information stolen.

In October, hackers initiated a denial of service attack that caused a massive Internet outage, leading to widespread disruption of commerce and usage among Americans who rely upon the Internet for a wide variety of transactions. The trucking industry is ever mindful of such threats, especially while the debate over autonomous vehicles unfolds. While the potential of automated trucks to improve highway safety and save lives is significant, so is the danger posed by cyber criminals and terrorists. ATA will continue to advocate for a policy framework on autonomous vehicles that will ensure public safety and reduce threats to our nation's infrastructure, while also encouraging innovation in this rapidly changing environment where the benefits of improving safety, reducing emissions and fuel burn, eliminating congestion and increasing productivity may ultimately reside.

The ATA also supports voluntary supply chain security programs that embrace stakeholder input, adopting best practices established by industry, and offering motor carriers valuable benefits in exchange for program participation. The sharing of information is yet another key component of the private and public sectors working in partnership to implement coordinated and integrated protective security measures.

Conclusion

Protecting our nation's critical transportation infrastructure is a key priority for the trucking industry, as it is essential to our nation's security and economic prosperity. Threats to our nation's roadways pose a danger to the motoring public and the security of our complex supply chain. The ATA remains committed to working with DHS to protect our highways from potential threats and mitigate the possibility of a truck conveyance from transporting or being used as a weapon. ATA has and will continue to actively participate as a member of the Highway and Motor Carrier Sector Coordinating Council to work with other industry stakeholders and our government partners to identify and implement solutions to improve the security of our nation's critical surface transportation infrastructure. Regulation for the sake of regulation, however, is not a solution. Security regulations should continually seek to effectively balance national security interests without hindering the efficient movement of goods throughout our economy by

placing undue burdens or costs on industry and subsequently, consumers. In doing so, our increasingly connected world and trucking industry requires a mindset where cyber threats to our nation's infrastructure can be just as consequential to public safety and our economy as physical attacks. The ATA stands ready to support Congress and DHS to be sure that enhanced national security and the unencumbered flow of commerce remain compatible priorities.