Before the

United States House of Representatives

Committee on Homeland Security, Subcommittee on Transportation Security

Statement of

Martin Rojas
Vice President, Security & Operations
American Trucking Associations

On

"Industry Perspectives: Authorizing the Transportation Security Administration for FY 2012 and 2013"

JULY 12, 2011

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

Introduction

Chairman Rogers, Ranking Member Jackson Lee, and members of the Subcommittee on Transportation Security, thank you for the opportunity to testify today on the Authorization of the Transportation Security Administration for FY 2012 and 2013. My name is Martin Rojas and I am Vice President for Security and Operations at the American Trucking Associations (ATA). Founded in 1933, ATA is the nation's preeminent organization representing the interest of the U.S. trucking industry. Directly and through its affiliated organizations, ATA encompasses over 37,000 companies and every type and class of motor carrier operation.

The trucking industry is an integral component of our economy, earning more than 80% of U.S. freight revenues and employing approximately 7 million workers in trucking-related jobs, including over 3 million commercial drivers. It is important to note that the trucking industry is comprised primarily of small businesses, with 97% of trucking companies operating 20 trucks or less, and 90% operating six trucks or less.[1] More importantly, about 80 percent of all U.S. communities depend solely on trucks to deliver and supply their essential commodities.

Highway Sector Supports Strong National and Economic Security

The U.S. highway and motor carrier sector has been defined by the U.S. Department of Homeland Security (DHS) as one of nineteen Critical Infrastructures/Key Resources (CI/KR). In 2006, various private sector highway related organizations established the Highway and Motor Carrier Sector Coordinating Council (SCC). The SCC works in partnership with public sector representatives established under a counterpart Government Coordinating Council (GCC) under the auspices of the Critical Infrastructure Protection Advisory Committee (CIPAC). The SCC and GCC have met for the past five years on a quarterly basis to share ideas and exchange information to improve the security of the Nation's highways. In addition to the SCC, ATA and its members participate in many industry and government-led initiatives focused on enhancing security and ensuring an open and efficient transportation system to deliver America's freight.

Today's hearing takes place just two months away from the tenth anniversary of the terrorist attacks of September 11, 2001. Since that day, the U.S. has undertaken various initiatives, both domestically and abroad, to prevent our enemies from planning and executing further terrorist attacks against us. From sending thousands of heroic men and women to fight abroad, to implementing laws, regulations and strategies at home to reduce the risk of terrorist attacks on U.S. soil, our country has mobilized an immeasurable amount of public and private resources to defeat our enemies and secure our country. To further mitigate the risks of future attacks, we must continue to strengthen cooperation among government agencies and private sector entities, improve coordination among government agencies at the federal, state and local level, and we must coordinate closely with our international trade partners and allies.

[1] American Trucking Associations, *American Trucking Trends 2011* (March 2011).

Established by the Homeland Security Act of 2002, DHS absorbed a number of federal agencies with the overall goal of improving coordination and intelligence sharing under a single federal entity. One of the main early objectives of DHS was to "unify authority over major federal security operations related to our borders, territorial waters, and transportation systems."[2] After almost a decade since the 9/11 terrorist attacks, it is appropriate that we review and assess the effectiveness of various security regulations and programs implemented to improve our Nation's security.

Implementing More Security Regulations Does Not Increase Security

As a key agency within DHS, TSA can have a positive impact by strengthening the partnership with private sector counterparts instead of seeking to increase the number of security regulations on industry. As a country, we will never fully eliminate the risk and potential for terrorist attacks. But the trucking industry believes that by working together, we can improve our Nation's security posture without sacrificing the need for an efficient and effective transportation system hampered by excessive security regulations and requirements.

At a recent hearing before this Committee, TSA Assistant Secretary John Pistole stated:

> *"TSA employs risk-based, intelligence driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism... TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our Nation's transportation system."*[3]

ATA fully agrees with Mr. Pistole's approach and stands ready to work with him, his TSA colleagues, and other federal agencies to improve the security and safety of the transportation sector. As we have encouraged past TSA leaders, we recommend that Mr. Pistole perform a review of all the security regulations and programs throughout the federal government that presently affect all transportation modes so that the agency has a better appreciation of the numerous security initiatives in place today. Because of the ubiquitous nature of the trucking industry throughout the transportation system, government mandates established to improve security in other modes or sectors have both direct and indirect impacts on trucking operations.

As this Committee considers the present security challenges faced by the highway transportation sector and how to mitigate these risks, it must also recognize that the trucking industry must also comply with a number of other regulations. In addition to security regulations, the trucking industry faces far-reaching and complex federal safety regulatory system. Increasing the regulatory burden on trucking companies as they are struggling to recover from the "Great Recession" does not help this critical industry improve its security nor its ability to grow its bottom line to spur economic growth and create more jobs. Since both government and private sector resources are finite, we

[2] President George W. Bush, "The Department of Homeland Security" Proposal, June 2002, p. 2 http://www.dhs.gov/xlibrary/assets/book.pdf

[3] Pistole, John S.; Statement before the Subcommittee on Transportation Security, June 2, 2011, p. 1

must choose carefully how we invest them to ensure our operations are secure, safe and efficient. 2222

At a hearing held on May 4, ATA expressed its gratitude to Committee members for their efforts and bipartisan leadership in addressing the continued multiplicity of Security Threat Assessments (STAs) that commercial drivers undergo to deliver America's freight. ATA and its members strongly support enacting the MODERN Security Credentials Act of 2011 and we look forward to Congress passing this important legislation. This issue remains ATA's top security policy priority for its potential to bring relief to millions of truck drivers and thousands of trucking companies from unnecessary and overlapping background checks and the resulting excessive costs.

In addition to multiple STAs, there are several government regulations and programs that require trucking companies to develop security plans, provide security training, develop en-route security procedures and incorporate security designs at company facilities, many with overlapping requirements, including the following:

- HM-232F: The Pipeline and Hazardous Materials Safety Administration (PHMSA), an agency within the U.S. Department of Transportation (DOT), promulgated HM-232 soon after the 9/11 attacks. HM-232 required companies transporting placarded loads of hazardous materials to develop security plans, security awareness training (both general and in depth), and en-route security requirements. In March 2010, PHMSA issued a final rule, HM-232F, refining the list of hazardous materials that require transportation security plans. Carriers that transport this security-sensitive subset of hazardous materials must perform risk-assessments of their operations and facilities, as well as provide in-depth security training to employees handling these hazardous materials. The Federal Motor Carrier Safety Administration (FMCSA) assures compliance with HM-232F during regular motor carrier visits where safety and security reviews are conducted. ATA supported PHMSA's rulemaking efforts to establish a risk-based approach to the transportation of hazardous materials.

- Customs-Trade Partnership Against Terrorism (C-TPAT): U.S. Customs and Border Protection (CBP) worked with industry immediately after the 9/11 attacks to develop a "supply-chain" security program to increase the security of international shipments imported into the U.S. by all modes of transportation, including trucks. Though C-TPAT is not mandated by statute and remains a "voluntary" security program, most carriers are required to become C-TPAT members by their C-TPAT certified customers/importers with international cross-border shipments from Canada and Mexico. The program requires participating companies to conduct risk-assessments, develop security plans, and implement specific security recommendations made by CBP Supply Chain Security Specialists (SCSS) to become certified and validated by CBP. As part of the Free and Secure Trade (FAST) program, Canada implemented a parallel program for imports called Partners-In-Protection (PIP) that incorporates similar requirements and a separate application and validation by Canadian officials.

- Certified Cargo Screening Program (CCSP): TSA's CCSP program requires participants to establish personnel security, physical security and procedural security requirements. The CCSP recognizes other STAs such as the Hazmat Endorsement, the Transportation Worker Identification Credential (TWIC) and the FAST card. As with other programs, CCSP has security requirements that are unique to the air cargo environment regarding technologies for screening cargo as well as chain of custody procedures.

ATA recognizes that higher-risk operating environments, such as air cargo or cross-border operations, have security requirements that must address specific risks associated with such operations. Because of this, a "one-size-fits-all" security approach is not a viable methodology for designing and implementing security requirements for an industry with such diverse operations. However, federal agencies must improve inter-agency communication and coordination to establish mechanisms that recognize basic "common requirements" in other security programs. In essence, if a CCSP compliant carrier is applying for C-TPAT certification, the carrier's application should undergo an accelerated C-TPAT certification and validation process.

Because several federal agencies already require motor carriers to implement security measures, the trucking industry does not support federal agencies, including TSA, implementing additional security regulations. Agencies that are considering implementing security requirements for the transportation of specific types of regulated commodities should first review all three of the above listed programs – HM-232F, C-TPAT, and CCSP – and consider if those programs meet their requirements for the secure transportation of their regulated commodities.

A positive example of the above scenario has been the implementation of the Chemical Facilities Anti-Terrorism Standards (CFATS) by DHS's Infrastructure Protection (IP) office. In early discussions between IP and transportation industry stakeholders, IP recognized that commercial drivers already undergo various STAs when transporting certain cargo, including chemicals, or when operating in certain environments. Thus, DHS considers the Hazardous Materials Endorsement (HME), TWIC and FAST screenings as compliant with the CFATS background check requirement. DHS also recognized the oversight authority of other federal agencies over chemical products, including DOT's regulations for the safe and secure transportation of hazardous materials. Thus, DHS stated that CFATS regulations would not supersede other federal agencies' chemical security requirements.

Transportation Worker Identification Credential: Focus on Outcome not on Output

ATA views the TWIC as a single instrument that can satisfy the needs of multiple agencies requiring background checks in various operating environments. The original concept of the TWIC, as espoused as far back as 2003, was to establish a single process, system and credential with broad application across multiple programs and transportation modes requiring workers to undergo a STA. This concept, known as "enroll once, use many", was included as one of the twenty key recommendations in the

Surface Transportation Security Priority Assessment prepared by the Transborder Security Interagency Policy Committee (IPC)[4] with industry input and support.

On May 10, 2011, the Government Accountability Office (GAO) released a study during a hearing held by the Senate Committee on Science, Commerce and Transportation to review the impact of the TWIC on port security. The GAO report found a number of security concerns with the implementation of the TWIC program, including the use of counterfeit TWICs to gain access to maritime facilities and the use of counterfeit identifications and fake identity data to apply and successfully obtain authentic TWICs. As a result, some Members of Congress are questioning if the TWIC has added any true value to the security of maritime facilities and to the entire transportation sector.

GAO has recommended a number of steps be taken by TSA and the U.S. Coast Guard (USCG), including the need for internal controls and effectiveness assessments to evaluate compliance with the program's original objectives. GAO also suggested that TSA analyze and determine what cost-effective measures can be taken to ensure that the program corrects the specific weaknesses found during the assessments, especially as they relate to identity fraud and the use of counterfeit TWICs. As a long-standing member of the TWIC private sector stakeholder group, ATA is concerned about the GAO findings.

As long as TWIC is simply used as a flash-pass it will be no more secure than a driver's license or any other photo identification. ATA urges this Committee to ensure TSA and USCG do not delay issuing a Final Rule for TWIC readers so that maritime facilities can use the technology established under the TWIC program to verify the identity of the card holder prior to accessing a facility. The technology embedded in the TWIC and the readers should help deter the use of counterfeit TWICs. TSA and the TWIC contractor must also take the necessary steps to ensure that TWIC applicants are presenting valid identification and biographical data upon application.

Information Sharing Trumps Security Regulations to Fight Terrorism

Last February, an alert trucking company employee prevented a terrorist plot involving explosives. A visiting Saudi student, Khalid Ali-M Aldawsari, was arrested in Lubbock, Texas for plotting to bomb several locations throughout the state, including the home of former President George W. Bush. Luckily, Mr. Aldawsari was arrested and his plans came to an end.

The incident reflected the positive effects of implementing appropriate security training for employees, while encouraging them to remain alert and report any suspicious activity or other concerns. In this case, a trucking company employee recognized and researched some of the materials listed in a package and alerted the company's security team. Federal law enforcement personnel were brought in and the would-be terrorist was eventually arrested when he tried to pick up the package.

[4] National Security Council, The White House, March 2010

As with other terrorist plots inside the U.S., this event garnered much media attention. However, among the various media outlets that covered the story, it was a CNBC story that truly captured the essence of what transpired:

> *In the end, it wasn't a TSA agent, a Homeland Security operative or an FBI agent who first spotted alleged terror plotter Khalid Ali-M Aldawsari. It was the employees of a private shipping company. According to the government, somebody at the shipping company called local police after becoming suspicious about a chemical package that Aldawsari was set to receive.*
>
> *Meanwhile, officials at the chemical company that sent the material called the FBI with their suspicions about Aldawsari—and later worked with an FBI agent who posed undercover as a company employee in dealings with the suspect.*[5]

What this story highlights is that all of us, government agencies, private industry and concerned citizens all share the responsibility for fighting terrorism. In the end, information sharing is the best and strongest tool that we have to stop potential terrorist plots and to fight terrorism at home and abroad.

As this event demonstrates, the private sector is an essential partner and part of the solution for combating terrorism. <u>We don't need more regulation, we need more cooperation</u>.

ATA and its members are presently participating in a number of information sharing initiatives to facilitate the flow of information and intelligence to improve the security posture of our industry. Initiatives involving the Homeland Security Information Network, the Office of the Director of National Intelligence, the FBI's InfraGard program, as well other federal, state and local efforts, are allowing industry to share information directly with the intelligence and law enforcement community. ATA urges this Committee to support such exchanges of information as a better alternative to establishing additional security regulations on an industry already over-burdened by safety and security regulatory mandates.

Conclusion

In the past ten years, many legislative, regulatory and voluntary efforts have been implemented to minimize the threat of another terrorist attack in the U.S. Though well intended, many initiatives have resulted in a multiplicity of overlapping and burdensome security requirements on trucking companies. Unfortunately, rather than augmenting the security of the transportation sector, the focus has been more on regulatory compliance rather than evaluating the impact of existing security requirements.

---

[5] "How Two Companies Stopped a Terror Suspect", CNBC.com; February 24, 2011; http://m.cnbc.com/us_news/41766933

ATA urges the Committee to consider the following recommendations as it deliberates TSA's Authorizations for FY 2012 and 2013:

- **Do not mandate more security regulations:** As an industry already heavily regulated by safety and security requirements, more security regulations will not improve security but will only increase the compliance burden on trucking companies;

- **Encourage information sharing:** Industry has embraced several initiatives by law enforcement and intelligence agencies to exchange information and increase our mutual understanding and information needs to improve our Nation's security posture;

- **Improve agency coordination:** Increase the communication and coordination among federal agencies that have established security requirements and programs that impact the surface transportation sector. TSA's Transportation Sector Network Management (TSNM) could play a role in such an initiative;

- **Ensure the TWIC reader rule is issued promptly:** TSA and the USCG must finalize the TWIC reader rule and ensure that the processes and systems are hardened to prevent counterfeiting and the use of false identity information to obtain a real TWIC.

Again, on behalf of ATA and its members, I thank you for the opportunity to share some comments regarding our industry's perspective and priorities as this Committee considers authorizing TSA for FY 2012 and 2013. I look forward to answering any questions you may have.