



Driving Trucking's Success

August 26, 2005

Via Facsimile (202) 395-5806

Office of Information and Regulatory Affairs
Office of Management and Budget
Attention: DHS-TSA Desk Officer

RE: Corporate Security Review
Vulnerability Identification Self-Assessment Tool-Transportation

Introduction

American Trucking Associations, Inc. (ATA) submits the following comments in response to the Transportation Security Administration's (TSA) two emergency information collection requests: Corporate Security Review (CSR) form for use in collecting information from surface transportation system owners and operators and Vulnerability Identification Self-Assessment Tool-Transportation (VISAT-T).

As the national trade association of the trucking industry, ATA is a united federation of motor carriers, state trucking associations, and national trucking conferences that promotes and protects the interests of the trucking industry. Directly, and through its affiliated organizations, ATA represents over 34,000 companies of every size, type, and class of motor carrier operation. The trucking industry shares the U.S. government's mutual goal of securing our nation's transportation system from acts of terrorism while ensuring our country's economic wellbeing.

ATA notes, however, that our comments on the CSR and VISAT-T are made without the benefit of having seen the actual CSR form or VISAT-T that are the subjects of these notices. ATA and the trucking industry, as well as other private sector representatives, continue to grow concerned with the various security programs and information and data gathering requirements that several U.S. government agencies have established without sufficient inter-agency communication and coordination.

Thus, ATA's primary goal in these comments is to encourage OMB to pursue the following two actions prior to approving TSA's, or any other U.S. federal government agency's, request for collecting corporate information from motor carriers:

1. Request that U.S. federal government agencies submit to OMB an inventory of their individual security programs that require industry to provide corporate information or data for compliance with both regulatory and non-regulatory security rules and programs. ATA is not aware of any such inventory at this time, though industry has requested a listing from the Department of Homeland Security (DHS) and other relevant government agencies; and,
2. OMB should then review the agency inventories and seek possible solutions that will address the duplicity of efforts by government agencies and industry in fulfilling such information requests. OMB is the entity within the executive branch responsible for budgeting and administrating federal agencies' resources and evaluating the effectiveness of federal agency programs. Therefore, OMB must ensure that both financial and human resources invested in developing federal government security programs and requirements are spent efficiently, do not result in duplicity of efforts, and that the costs of developing and complying with such requirements do not exceed the real benefits.

Trucking Industry and Security

In today's modern supply chain, trucks are an ubiquitous fixture throughout our nation's economy. The trucking industry is a complex industry comprised of different operational models, such as, full truckload, less-than-truckload, intermodal, tank truck, food and agriculture, munitions carriers, package carriers, and other specific sectors. Each of these trucking sectors have fine-tuned their business models and adopted strategies that produce the most efficient, cost-effective, safe, and secure movement of goods.

But perhaps most important is the fact that the U.S. trucking industry is predominantly comprised of small businesses that form the backbone of our transportation system. As of July 2004 (see Attachment II for more statistics):¹

- 524,309 interstate motor carriers were on file with the Federal Motor Carrier Safety Administration (FMCSA)
- 95.9% of carriers operated 20 or fewer trucks
- 87.3% of carriers operated 6 or fewer trucks

ATA cites these statistics to emphasize the significant role small businesses play in the trucking industry. The increasing levels of security requirements are having an impact on motor carriers of all sizes and their capabilities to provide specific types of operations and services. Motor carriers must not only deal with increasing security requirements for certain types of operations, but must also satisfy a variety of regulatory requirements by federal agencies, such as safety regulations under the U.S. Department of Transportation (DOT). Small motor carriers are less able to absorb new increasing costs for compliance.

¹ American Trucking Associations, *American Trucking Trends*, 2004

Many motor carriers have indicated their intent to no longer transport certain types of cargo due to the increasing costs of background checks on their drivers and their inability to find drivers willing to pay for and undergo security threat assessments. The trucking industry must presently comply with a variety of background checks for drivers, for developing security plans, and for providing security training to drivers and other employees. (Attachment I shows the various background check requirements). Motor carriers of all sizes provide various types of operations, such as transporting hazardous materials, food products, and serving maritime and air terminals, all of which now require, or will require, security requirements in the near term.

Overlapping Agency Programs

Various government agencies have placed numerous security requirements and regulations on the trucking sector with the objective of strengthening the overall supply chain from acts of terrorism. The proliferation of new regulations and programs by different agencies has made our industry increasingly concerned with the duplicative programs and processes that now exist. Duplicative processes serve only to frustrate industry by creating unnecessary cost burdens on large and small businesses and offer no added security benefit. Agencies within DOT, such as Federal Motor Carrier Safety Administration (FMCSA) and the Pipeline and Hazardous Materials Safety Administration (PHMSA), as well as the Department of Homeland Security (DHS) agencies, such as U.S. Customs and Border Protection (CBP), and the Transportation Security Administration (TSA), currently have in place security requirements for motor carrier operations including enhancements to security plans, security training, safety permits, security inspections, and driver and personnel security.

It is imperative that government agencies coordinate/consolidate overlapping requirements and data to relieve carriers from redundant processes and minimize the significant cost implications to our industry. OMB must direct agencies to coordinate and eliminate redundancies in the processes by which motor carriers provide corporate information for participation in security programs. Alternatively, OMB must provide guidance, or develop a coordinated policy, by which federal agencies can accept a company's information for participation in another agency's program for their own security programs. Corporate security reviews are not a new concept for the trucking industry in the post 9/11 environment. Following, ATA describes federal agency requirements that request motor carriers to provide corporate information.

FMCSA's Security Contact Review Program

Shortly after 9/11, FMCSA initiated Security Sensitivity Visits (SSV). SSVs are on-site meetings between FMCSA or state investigators and trucking company officials to assess a company's security practices, identify security gaps, and offer recommendations to improve any deficiencies noted. The SSV guidelines recognize the operational differences among carriers and allow investigators flexibility when providing recommendations that are suited to the size and scope of the operation. Between October 2001 and January 2002 FMCSA conducted over 36,000 motor carrier SSVs.

In March 2003, the Research and Special Programs Administration (RSPA), now PHMSA, which has regulatory authority over hazardous materials transportation, published HM-232, a final rule with the objective of enhancing the security of hazmat transportation. HM-232 requires hazardous materials transporters to develop and implement security plans and provide employee security training which specifically focuses on potential terrorist or criminal threats. The Highway Watch®² security awareness training program, which has now trained over 140,000 highway professionals, is an accepted program for compliance under this rule. To ensure that hazmat carriers are complying with the security plan and training requirements mandated under HM-232, FMCSA began including SSVs as part of the compliance review process.

FMCSA began the enforcement phase of the SSVs with the establishment of the Security Contact Review (SCR) which evaluates a carrier's security performance on the following elements: Security Assessment, Security Plan, Personnel Security, Unauthorized Access, En Route Security, Security Plan Administration, and Security Training. An FMCSA investigator conducts an in person SCR on hazmat transporters, completes an SCR form with security recommendations, and has authority to write citations to carriers who fail to properly implement the HM-232 security plan and training requirements.

CBP's C-TPAT/FAST Program

C-TPAT/FAST is a voluntary, joint government-business initiative to strengthen the overall supply chain and border security by requiring participating companies to ensure the integrity of their security practices. Trucking companies that become C-TPAT/FAST certified not only create an additional layer of security to the supply chain but receive benefits such as reduced border inspections and use of dedicated crossing lanes which enhances carrier productivity and efficiency. To qualify as a C-TPAT/FAST participant, companies must meet strict security guidelines as established by CBP in the following areas: procedural security, physical security, personnel security, security training and threat awareness, physical access controls, manifest procedures, conveyance security, conveyance inspection procedures, information technology security, and business partner requirements.

To participate, companies first conduct a comprehensive self assessment in the above key areas which CBP evaluates and reviews with the applicant company. CBP works with the applicant to identify potential security gaps and offers recommendations for improvements that will qualify within CBP guidelines. Once CBP approves the carrier's

² Funded by the U.S. Department of Homeland Security and administered by the American Trucking Associations, Inc., Highway Watch® trains highway transportation professionals to assist in the safety and security of the United States and the highway critical infrastructure by observing, assessing, and reporting safety and security incidents that may pose a threat. Reports of a security nature are also forwarded to the Highway Information Sharing and Analysis Center which shares any resulting analysis with federal officials co-located at the Transportation Security Operations Center. Highway Watch® has four main program components: (1) Training, Recruitment, and Outreach; (2) Operations Coordination; (3) Information Sharing and Analysis; and (4) Emergency Planning and Education. To date, more than 140,000 individuals have been trained with tens of thousands more to be trained by year's end.

security plans and practices, the company becomes a certified C-TPAT/FAST partner and is entitled to the benefits associated under the program.

A further CBP validation process is then conducted to ensure the C-TPAT/FAST participants have implemented all required security measures outlined in their security profile. This validation process includes an on-site visit by CBP personnel to conduct an extensive and thorough examination of the company's security practices.

TSA'S Corporate Security Reviews

TSA's request for approval and processing of a CSR form to collect information from motor carrier companies raises some redundancy concerns given that motor carriers already provide this information as described above under FMCSA's SCR and CBP's C-TPAT/FAST program. These programs conduct on-site visits to assess a company's security posture, identify vulnerabilities in their operations, and recommend countermeasures that can improve overall security.

The purpose of the CBP and FMCSA reviews is to provide the agencies with an understanding of each carrier's ability to protect its critical assets, aid in developing security program baselines, establish best practices for the trucking mode and strengthen the overall supply chain. This is also the stated purpose of the TSA information collection request. ATA questions whether TSA's proposed CSR collection method of conducting lengthy on-site motor carrier operation reviews is the best way to access information that has already been collected by, and is currently available from, other agencies. Again, OMB should set guidelines for agencies to eliminate repetitive CSRs and avoid developing duplicative CSR forms for security evaluations on potentially the same companies to collect the same data.

TSA estimates that conducting 75 annual CSRs on surface transportation owner/operators, with a goal of two per month on motor carrier operators, will capture sufficient information necessary to perform data analysis which can ultimately be used to ascertain baseline security standards for industry. TSA also indicates that they do not intend to collect information from small businesses or other small entities at this time. ATA believes that using currently available FMCSA and CBP security plan data taken from tens of thousands of motor carriers across a broad spectrum of the industry captures better data for analysis than does TSA data collected from 24 large carriers annually. While ATA recognizes that TSA's CSRs are conducted voluntarily they are, nonetheless, redundant reviews that must be coordinated with other agencies.

Cost Burden

To collect the required information, TSA modal experts must first review the motor carrier's security plan documents, tour the carrier's facility and interview the owner/operator's staff and contractors on 11 security planning topics: threat assessments, vulnerability assessments, security planning, credentialing, secure areas, infrastructure protection, physical security countermeasures, cyber security, training,

communications, and exercises. TSA anticipates it will require three modal experts spending two, eight hour days at the motor carrier facility to gather sufficient information necessary to accurately complete the CSR form. During this two day process, respondents will provide TSA access to multiple employees to escort TSA officials, respond to document requests, give tours of their facilities, and answer questions.

Given the above requirements, ATA disagrees that the total annual cost burden to respondents is \$0.00. Respondents will incur direct labor and other associated costs necessary to comply with the collection information request. When using TSA's 1200 annual hour burden estimate, these costs can add up to a significant annual cost burden on respondents. ATA recognizes that the motor carriers who participate in the CSRs do so voluntarily; however, a true cost burden cannot be ignored.

TSA's Vulnerability Identification Self-Assessment Tool – Transportation (VISAT-T)

Again, it is difficult to fully comment on TSA's online self assessment tool without access to the trucking module which is not yet available for public review. Should TSA implement the VISAT-T, ATA, as a key stakeholder, offers to review and provide feedback on the trucking module prior to its release.

ATA's concerns with the VISAT-T are the same as we have with the CSR. As discussed above, FMCSA's SCRs and CBP's C-TPAT/FAST programs require companies to conduct a comprehensive security self assessment as a first step in the review process. Both programs, recognizing the complexity and diversity of the transportation system, determine appropriate security measures based on risk analysis and allow for flexibility and customization of carrier security plans given the individual carrier's unique operating characteristics. The notice states that TSA's VISAT-T intends to incorporate the same elements. ATA questions the value of TSA developing a new self assessment tool as the methodology to collect security related data on carriers which already exists within other agencies.

It is also noted that the VISAT-T notice did not state that TSA would treat information collected from respondents as sensitive security information as described in 49 CFR parts 15 and 1520. It is critical that TSA, or any government agency, consider proprietary company information provided through the self assessment process as SSI.

Unclear Goal of CSR and VISAT-T

It is unclear to ATA what the information collected under these two programs can provide to TSA that does not currently exist within other government agencies or how government will use the information to provide added security benefit to the transportation system. ATA requests that TSA more clearly define the purpose of the programs and address how the data collected for the CSR and VISAT-T can enhance security, based on risk analysis, above and beyond current initiatives.

Conclusion

It is imperative that OMB recognize the various security programs already in existence to avoid approving redundant information collection requests and ensure the best use of government and industry resources.

ATA appreciates the opportunity to provide comment on TSA's CSR and VISAT-T information collection request and offer the following recommendations for your consideration:

- Request that federal government agencies submit to OMB an inventory of existing security programs that require industry to provide corporate information and data. This inventory is necessary to avoid approving redundant information collection requests.
- Consolidate/Coordinate information collection with other agencies to reduce the number of duplicative CSRs and self assessments conducted on motor carrier operators.
- Adhere to risk-based principles when determining compliance standards to ensure the associated requirement costs are commensurate with the realized security benefit.
- Recognize that varying sectors within the industry have unique business models and applying a one-size-fits-all approach will do little to aid the security mission.
- Acknowledge the cost implications of duplicative processes on the trucking industry which is predominantly comprised of small businesses.

ATA and the trucking industry remain strongly committed to securing our nation's transportation system from acts of terrorism and continue to be strong proponents and partners in ensuring our national security as well as economic wellbeing. We continue to offer our industry expertise and input on security issues that affect our industry. Please feel free to contact Jeanne Dumas at ATA, jdumas@trucking.org or 703-838-1703 should you wish to further discuss these comments.