

**April 22, 2003**

**Comments Submitted to: Subcommittee on Energy Policy, Natural Resources & Regulatory Affairs**

**Comments Submitted by:**

Stephanie Williams  
Vice President  
California Trucking Association  
3251 Beacon Blvd.  
West Sacramento, CA 95691  
(916) 373-3548

**Subject:** CTA Position and Items of Concern on Port Security

**1: Definition of facility under the port area security plan.**

In some ports, trucking terminals are located on port property. Even though their function is not of a “marine” nature, these terminals will dispatch equipment to deliver cargo and containers in an out of the “maritime environment.” While the portion of the operation that interfaces with maritime operations will need to take into account the requirements of the port security plan, clearly many of the International Maritime Organization (IMO) security protocols do not directly apply to truck operations. Facilities located adjacent to navigable waterways may be designated under the port security plan. If a trucking terminal (on private, non-port property) is located near a critical maritime infrastructure, such as a dock, or could be used to launch an attack on shipping, such as a fuel operation located next to a critical ship canal, these facilities could be required to participate in the port security plan, and to submit a security plan for approval by the captain of the port.

Potential inter-agency inconsistencies, planning requirements and needs must be recognized and reconciled to avoid conflicting and potentially disruptive requirements.

**Concern 2. THERE SHOULD BE ONLY ONE BACKGROUND CHECK OF A TRUCK DRIVER AGAINST THE FEDERAL DATABASES THAT IS UNIVERSALLY APPLICABLE AND RECOGNIZED.**

- A truck driver today may potentially be subject to background checks against the same NCIC database under the following regimes: 1) aviation; 2) ports; 3) carrying hazardous materials; 4) carrying explosives; 5) carrying goods for the Department of Defense; 6) border crossings under the voluntary Free and Secure Trade (“FAST”) program; and 7) numerous state and local criminal background check requirements (e.g. ports in Florida and South Carolina)
- It is costly and duplicative to check the same driver against the same database; however we support periodic checks/renewals (i.e., requiring one check every three years)

- The federal background check for truck drivers must preempt all other state and local requirements

### **3. THE BACKGROUND CHECK MUST BE QUICK, EFFICIENT AND COST-EFFECTIVE**

- Earlier estimates by FMCSA regarding implementation of the USA PATRIOT Act predicted the turnaround time for a hazmat endorsement to be between 3-6 months
- Many states do not even allow a person to apply for renewal of a hazmat endorsement more than 30-60 days out (a chart listing state requirements is attached); thus any greater delay would put drivers out of jobs
- The states have neither the infrastructure nor the funds to put in place an efficient system
- Private sector models, including the aviation and banking industries, turn around NCIC checks in 4-7 days
- Any background check regulation should be flexible enough to allow private sector solutions

### **4. THE DISQUALIFYING CRITERIA SHOULD BE CLEAR AND CONSISTENT AND THE RESULTS OF THE BACKGROUND CHECKS COMMUNICATED TO THE EMPLOYER.**

- Under the USA PATRIOT Act, the disqualifying standard is if the Secretary determines the applicant poses a security risk; what does that mean?
- When the Secretary makes a determination that the driver poses a security risk, the driver's employer should be informed concurrently as to why
- THE EMPLOYER, AT A MINIMUM, SHOULD BE AFFORDED LIABILITY PROTECTION FOR EMPLOYMENT DECISIONS ARISING OUT OF A MANDATED BACKGROUND CHECK

### **5. THE ONLY WORKABLE SOLUTION APPEARS TO BE TYING THE BACKGROUND CHECK TO THE ISSUANCE OF A TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL AND NOT A DRIVER'S HAZARDOUS MATERIALS ENDORSEMENT.**

- There are background check requirements at ports and airports; not all drivers carrying goods there have hazmat endorsements to their CDLs
- Many shipper-customers are requiring second forms of identification; a TWIC could become the universally accepted standard

- The CDL was always aimed at a driver's safety fitness; the TWIC could be developed with security fitness in mind

## **6. IMPLEMENTATION OF THE BACKGROUND CHECK RULE MUST NOT DISRUPT THE FLOW OF COMMERCE.**

- Any background check rule should be phased in over a reasonably sufficient period of time to ensure compliance is feasible given the volume of drivers that will be subject to such rule
- Drivers must be permitted to continue driving while the background check is being conducted
- The impact on the trucking industry's ability to continue hauling the Nation's freight must be carefully considered
- Qualifications for facility security officers in "non-marine" facilities must take into account the relationship between trucking and the maritime environment.

## **7. THE TRUCKING INDUSTRY SHOULD BE AT THE TABLE**

While it makes sense for marine facilities to have security staff with expertise in the IMO security protocols, it does not make sense to require a land-based facility like a motor carrier to have marine/IMO security expertise. The fact that trucking operations require different skills and knowledge must be reflected in the security requirements placed on their facilities, and the associated port security committees and plans. Intermodal motor carriers must have a seat on each local port security committee.

At many ports it is quite likely that more trucking personnel enter ports with greater frequency and numbers than any other category of persons, including port employees themselves. Accordingly, their perspectives and expertise are crucial to assure development and implementation of a successful security plan, and at the same time, maintain the efficiencies of the intermodal freight system that yield universal benefits. To assure proper localized representation, a state-based motor carrier industry organization, or its designee, should hold this seat.

## **8. System Interoperability – The personnel credentialing system at one port should match all other ports. Resulting interoperability is fundamental to intermodal freight systems' efficiencies, and vital to governments' intelligence and security objectives.**

Myriad data collection and processing systems are currently available for both freight tracking and secured facility access. Most of them are proprietary and many have associated subscription fees. To move freight throughout the country, motor carriers and others often must subscribe to several different systems. This is equivalent to having to use multiple transponders. If government develops newly required systems,

the picture only gets worse. Government leadership and responsiveness to private sector stakeholders is the key to achieving interoperability across all freight systems.

A perfect example of how not to implement security objectives and related technology is found in Florida. Prior to September 11, 2001, the Florida legislature mandated that each of their 14 marine ports establish an identification card system with an associated criminal background check. Void in this plan were any requirements for interoperability, so that the system at one port was interoperable with any other port. This was done in spite of the fact that the Executive Director of the Florida Trucking Association cautioned and pleaded with lawmakers to make the system interoperable. The legislature ignored industry. As a result, each truck driver seeking access to all 14 ports must fill out 14 applications, pay 14 processing fees, get fingerprinted 14 times, be in possession of all 14 cards, and renew them periodically. This means that all 14 applications from a solitary driver are sent to the same Florida law enforcement agency for processing, and for that lone driver, the FBI is burdened 14 times to conduct a fingerprint and background check, and return 14 reports to the Florida agency. The resulting burden to the driver is truly ridiculous. Moreover, American businesses struggling to be globally competitive are reliant on cost-effective intermodal freight service. Ultimately, they suffer from the cost of this boondoggle too. But perhaps the most unacceptable result from ignoring interoperability, is that to do so, creates security system redundancies that enlarge the potential for security failures.

By stark contrast, the trucking industry commends the United States Coast Guard for seeking the participation of the private sector.

**9. Port Driver/Worker Credentialing System – The trucking industry strongly supports an interoperable Port Worker’s Identification Card, which works in an open-architecture environment.**

The technology of the Port Worker’s Identification Card should closely resemble the concept developed by the Credentialing Direct Action Group. The day after September 11, Secretary Norm Mineta organized the National Infrastructure Security Committee (NISC), and charged that group with fortifying America’s infrastructure against terrorists’ nefarious aims. The NISC formed several subgroups where the trucking industry is well represented. Under the NISC, the Credentialing Direct Action Group developed the conceptual framework for a Transportation Workers’ Identification Card. This concept generally incorporates protocols, open architecture, protection of confidential personal and corporate information, and technical features that result in an efficient and interoperable system vital to truckers’ interests. In its Federal Register Notice on December 30 of 2002, the USCG (at page 79750) states its intention to incorporate these concepts to provide secured personnel access to security sensitive port areas and facilities. America’s trucking industry strongly supports USCG in this objective.

*Technology Selection Criteria:* When good security proposals also portend increased economic efficiencies, this helps to offset costs (both start-up and perpetual costs). The trucking industry astutely understands the need for accurate, dependable and secure driver credentials. Increasingly, motor-carriers’ customers are pressuring them to develop a system that not only identifies a driver as holding a valid CDL, but also confirms who he works for and that he or she is authorized to pick up a load. The

features associated with the Credentialing Direct Action Group meet these criteria. Accordingly, motor carrier customers could voluntarily adopt the same technologies for security at their places of business. The effect would be to drive down costs through efficiencies of scale.

#### **10. Data Privacy must be protected.**

The trucking industry, like the other three freight modes, does not collect freight data and information without a clear purpose. In almost all cases it is collected as part of conducting business in a competitive environment. Consequently, while there is a substantial amount of freight data, much of it is proprietary. The trucking industry supports security programs but government, and the systems they propose building, must be extremely sensitive about protecting data.

Any drivers' personal data, and business' proprietary and confidential information, must enjoy robust protection by the system. Laws must severely punish criminals unlawfully obtaining or using this information, and include far-reaching financial sanctions and lengthy incarceration.

#### **11. Mandated Vs. Performance-Based Systems: Government should focus on functional needs and let the industry decide how to meet and deliver those functional requirements.**

Among other objectives, terrorists seek to destroy our economy. Government, with the assistance of industry, must make every effort to effectively build sufficient security infrastructure without being so costly or cumbersome as to destroy the economy it seeks to protect. USCG should be praised for its deliberate and copious efforts to develop optimum systems, procedures and policies. In this vein, it is important to understand that the trucking industry has already invested in highly sophisticated and very expensive systems. Since September 11, thousands of government agencies and private businesses have been waiting for Congress, and the agencies it controls, to provide leadership to specify the open architecture and protocols necessary and antecedent to further investment. The intervening uncertainty has been extremely frustrating to all stakeholders. Key to America's success in thwarting domestic terrorism is to shun mandates reliant on proprietary vendors, and to engage in industry and government partnerships to jointly analyze, field test, and determine security programs.