Technical Report Documentation Page

1. Report No. SWUTC/10/473700-00074-1	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle State Commercial Vehicle Security Enforcement: Operations, Technologies, and Barriers		5. Report Date August 2010 6. Performing Organization Code
7. Author(s) Alison J. Conway and C. Michael Walton		8. Performing Organization Report No. Report 473700-00074-1
9. Performing Organization Name and Address Center for Transportation Research University of Texas at Austin 1616 Guadalupe Street Austin, TX 78701		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTRS99-G-0006
12. Sponsoring Agency Name and Address Southwest Region University Transportation Center Texas Transportation Institute Texas A&M University System College Station, TX 77843-3135		13. Type of Report and Period Covered 14. Sponsoring Agency Code
15. Supplementary Notes Supported by a grant from the U.S. Department of Transportation, University Transportation Centers Program		

16. Abstract

This report details the results of a survey of state enforcement agencies concerning past, present, and future enforcement practices and advanced technology use for commercial vehicle security, as well as recommendations for future improvements. The study examines practices in 19 states, including 7 land border crossing states and 11 states with one or more major marine ports of entry. Current technology applications, future needs, and past and existing barriers to implementation are all identified. The study also examines both successes and needs for cooperation between federal, state, and industry stakeholders. Particular focus is also placed on identifying changes that have occurred since 9/11.

17. Key Words	18. Distribution Statement
Commercial Vehicles, Enforcement, Security, ITS	No restrictions. This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161.

19. Security Classif. (of report)	20. Security Classif. (of this page)	21. No. of pages	22. Price
Unclassified	Unclassified	66	

STATE COMMERCIAL VEHICLE SECURITY ENFORCEMENT: OPERATIONS, TECHNOLOGIES, AND BARRIERS

by

Alison J. Conway
C. Michael Walton

Research Report SWUTC/10/476660-00064-1

Southwest University Region Transportation Center
Center for Transportation Research
University of Texas at Austin
Austin, Texas 78712

August 2010

ACKNOWLEDGEMENTS

The authors recognize that support for this research was provided by a grant from the U.S. Department of Transportation, University Transportation Centers Program to the Southwest Region University Transportation Center.

DISCLAIMER

ABSTRACT

This report details the results of a survey of state enforcement agencies concerning past, present, and future enforcement practices and advanced technology use for commercial vehicle security, as well as recommendations for future improvements. The study examines practices in 19 states, including 7 land border crossing states and 11 states with one or more major marine ports of entry. Current technology applications, future needs, and past and existing barriers to implementation are all identified. The study also examines both successes and needs for cooperation between federal, state, and industry stakeholders. Particular focus is also placed on identifying changes that have occurred since 9/11.

EXECUTIVE SUMMARY

Since 9/11, and even before, truck security has been primarily considered a responsibility of shippers and the carriers who move their goods through the highway network. However, securing highway freight transportation in the U.S. requires participation from a number of stakeholders, including federal agencies, state agencies, shippers, and carriers. The roles of shippers, carriers, and the federal government are relatively well-defined. Shippers must ensure that goods are secure before being loaded onto a truck and are resistant to tampering. Carriers are responsible to ensure that goods safely and securely reach their destination, without being tampered with en route. The federal government develops regulations that are implemented and enforced by both federal and state authorities. However, the specific roles of state agencies are more difficult to identify. In some states, it is unclear what agency (if any) is even responsible to ensure the security of trucks on its highway network.

The purpose of this research is to examine state authority operations and technology use for the purpose of securing commercial trucks. In order to gain a comprehensive understanding of state authority roles, responsibilities, and operations, a survey was developed and distributed to state authorities identified as the primary agency responsible for truck security. Responding agencies included Departments of Transportation, Departments of Motor Vehicles, and State Law Enforcement Agencies. Specific topics of interest in the survey included current operations and technology use, changes since 9/11, remaining needs, and barriers to improvements.

Current security-related operations include credentialing, size and weight enforcement, vehicle inspection, cargo inspection, and vehicle tracking. These operations are detailed in Chapter 2. Activities range from manual vehicle inspections at traditional static weigh stations to tracking of hazardous materials shipments using global positioning system (GPS) technologies. Since 9/11, a number of operational changes have been implemented; these are detailed in Chapter 3. Recognized changes include increased training for inspectors, increased numbers of inspections, and increased numbers of staff (although increases have not been uniform across states and have been limited by budget realities and other barriers). A number of states have also introduced more advanced methods of cargo inspection, including radiation and chemical/biological

weapons detection since 9/11. These additions have been heavily focused in states with major land border crossings. Most states have also developed specific procedures for inspection during an elevated terror alert.

The survey identified very little comprehensive truck security planning at the state level; only a few states were found to have developed comprehensive plans. Communications between relevant state, federal, and industry stakeholders were also found to be sparse; these findings are also detailed in Chapter 2. Both the American Trucking Associations (ATA) and Commercial Vehicle Safety Alliance (CVSA) have provided informal forums for information sharing, but in general, interagency cooperation is lacking. Half or slightly more than half of states have coordinated efforts with state trucking associations and FMCSA. About one third of the surveyed states have coordinated with Customs and Border Patrol (CBP) or the Transportation Security Administration; however these states are concentrated at the land borders. Survey respondents did identify communications improvements, especially with CBP at land border crossings and between states, since 9/11. These improvements are discussed in Chapter 3.

Despite recognized operational, technology, and communications improvements, respondents have identified many remaining needs. These needs and the barriers that have prevented their being addressed are discussed in Chapters 4 and 5. States are still struggling to provide adequate staff, facilities, and hours of operations. New technology implementations are still needed, and further communications improvements are required. A number of barriers have prevented improvements from being made. Fiscal constraints have limited construction of inspection stations, inspection hours, staff sizes, and technology implementation. Technology implementations have also been limited by lacking support infrastructure. Concerns about technology limitations, data and system security, and driver and carrier privacy were also recognized by some states as barriers to advancement, although these concerns were fewer than expected. Overall it is clear that truck security practices of state authorities vary heavily between states. Although some improvements have been made since 9/11, a number of needs and barriers that must be overcome remain to achieve desired security improvements.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Throughout history, terrorist organizations have employed elements of transportation systems both as high-visibility targets resulting in severe loss of life and as weapons capable of causing severe damage. Incidents have not been limited to individual transportation modes. Roads and bridges have long been strategically targeted to prevent the movement of goods and people. Cars and trucks have been employed as both moving and stationary incendiary devices. Public transportation systems, including both trains and buses, have been targeted by bombers, and commercial airliners have not only been targeted, but also turned into weapons themselves, as occurred on 9/11.

While the threat of terrorism to transportation is not new, both government and public interest in the security of America's domestic transportation system has increased tremendously since 9/11. Both governments and system operators have been forced to examine their practices and to implement changes to ensure the security of vehicles, passengers, and cargo. As a primary target of the 9/11 terrorist attacks, the commercial airline industry has been the focus of centralized federal regulation. The Transportation Security Administration (TSA) defines and constantly reviews and updates procedures that must be followed at all US airports. For other modes of transportation, changes in both practice and technology have been implemented at a much more localized scale, with little coordination between stakeholders.

Areas of focus in recent transportation security research for both passengers and freight have been primarily driven in response to major events. In the aftermath of 9/11, there has been rapid advancement in the technologies available for passenger and cargo security at airports. Attacks on public transportation systems in London and Madrid have driven research into practices and technologies for securing public transportation systems. Hurricanes Katrina and Rita inspired focus on emergency response and management. The Dubai World Ports scandal brought interest in the security of containerized and bulk cargo entering the U.S. from international origins, and escalations in violence along the southern border have driven calls for improvement in the security of both passengers and cargo entering the US through land border crossings.

Securing the nation's increasingly congested freight transportation network remains vital, as it may provide a means of entry or facilitation to any number of potential threats. Weapons, drugs, other dangerous materials, even terrorist themselves could be smuggled into the country through its trade lanes. Misuse of hazardous materials (HazMat) shipments, prevention of a necessary HazMat delivery, or tainting of an agricultural shipment could initiate serious social health incidents. Interruption of traffic flow at a critical location could also lead to considerable economic damages.

Industry trends indicate that securing the nation's land freight transportation system will only become more difficult in future years. As growing domestic and international freight traffic moves commercial vehicles off of major highways where the majority of enforcement activities are currently performed, more vehicles may evade inspections (*1*). Additionally, rising fuel costs may limit the resources available to carriers for security purposes. Already, a huge amount of truck traffic moves across the borders with Canada and Mexico. Although Mexican vehicles are not currently permitted to travel beyond a very limited area, if the 1994 North American Free Trade Agreement is fully implemented, truck traffic from the south could potentially increase considerably. While considerable research and policy focus has been given to security practices at marine ports, where container and bulk cargo enters the US from international origins, it is clear that increasing inspection practices at these locations could lead to intolerable delays. As a result, the vast majority of cargo entering the US through marine terminals is not directly inspected. This cargo will eventually make its way to the nation's highway network. Even freight carried out of the port by rail is likely to be transferred by a truck at some stage before it reaches its final destination.

So far, the government role in securing trucks has been limited compared to other modes. The security of domestic truck freight in the US has been primarily left up to the shippers and carriers responsible for the transportation of goods. Many carriers, particularly large carriers, employ a number of technologies to track their assets; these include both tractor on-board GPS units and trailer tracking units. These systems are useful in identifying security threats when monitored routes deviate from intended or approved locations. Carriers also maintain on-board communication systems with drivers, via radio and cellular connections that allow for quick

identification and reporting of potential threats. Although it was defunded in 2008, the American Trucking Associations' (ATA) Highway Watch ® program provided driver security training and a call in center for truck drivers to report suspicious activities observed on the highway network. Recent studies have examined security practice and the use of advanced technologies for commercial vehicle security by carriers (*2*). "Homeland Security and the Trucking Industry," a 2005 report completed by the University of Minnesota and the American Transportation Research Institute (ATRI), discusses the finding of several studies, including a pre-9/11 technology survey performed by the ATA, a 2003 ATRI carrier technology survey, and a 2004 ATRI study of agricultural carriers (*1*). FMCSA has also performed several studies focusing on technology applications for HazMat security, including the "Field Operational Tests" of various security technologies (*3*).

Shippers also bear responsibility in ensuring the integrity of the goods that they ship both domestically and internationally. To prevent losses of goods and tampering, shipping yards are secured whether through traditional security methods or through application of advanced fencing and monitoring systems. Shipping containers can also be electronically sealed to ensure that the contained cargo has not been tampered with en route from the destination (*4*).

Government efforts to secure truck freight transportation in the US have been more limited. Federal efforts have been primarily focused at both land and marine ports of entry. For example, customs authorities have implemented new regulations as well as increased technology use at ports of entry, such as carrier pre-screening (*5*) and Vacis detectors (*6*). Since 9/11, federal authorities have also demonstrated commitment to securing domestic hazardous materials (HazMat) shipments, both through the testing of GPS-based tracking systems (*3*,*7*) and through changes in driver regulation, such as implementation of the US Patriot Act, which requires all drivers seeking HazMat endorsement on their licenses to undergo a security threat assessment performed by TSA (*8*). In the federal government, the Transportation Security Administration (TSA), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Federal Motor Carrier Safety Administration (FMSCA), and the Federal Highway Administration (FHWA) must all play a role in securing drivers, vehicles, and cargo traveling on

the nation's freight highway network, as well as the infrastructure critical to continued flow on that network.

Many state enforcement agencies have also increased operations, improved training programs, and invested in new technologies; however, little recent research has examined the changes in practice and technology that have occurred at the state or local government level to secure truck freight. Just like at the federal level, in many states, various agencies are responsible for commercial vehicle security, including but not limited to state Departments of Homeland Security (DHS), state police departments and Departments of Public Safety (DPS), and state Departments of Transportation (DOT) and Departments of Motor Vehicles (DMV). As a result, it has been difficult to identify not only the practices and technologies employed for commercial vehicle security and changes that have occurred since 9/11, but also to identify the responsible agencies. The goal of this research is to comprehensively examine current security operations and advanced technology use by state agencies primarily responsible for commercial vehicle security.

In order to gain an understanding of CV security practices across a wide variety of states, a survey was developed for distribution, and the survey was completed in the summer of 2005. Initial state contacts were identified with the help of the Commercial Vehicle Safety Alliance (CVSA). Surveys were distributed in both online and paper formats via email and fax. The 19 responding agencies included two DOTs, two DMVs, and 15 state police, highway patrol, DPS, or vehicle enforcement agencies. Respondents included states in various regions of the country, including seven states with international land border crossings and ten states with one or more major marine ports of entry (Figure 1).

Figure 1. Participating States

The results of this survey provide answers to a number of fundamental questions about commercial vehicle security enforcement at the state level:

- *Who* are the agencies responsible for ensuring the security of commercial vehicles operating on the nation's highway network?
- *What* types of enforcement and inspection are being performed?
- *When* and how often are these inspections performed?
- *Where* on the highway network are inspections performed?
- *What* technologies are currently in use or desirable to state enforcement agencies?
- *How* do state agencies communicate with federal, state, local, and industry stakeholder concerning commercial vehicle security?
- *How* have security practices and technologies changed since 9/11?
- *What* barriers have prevented improvements?

The following chapters detail the results of this survey and provide a discussion of state enforcement practices and technology implementations for commercial vehicle security.

CHAPTER 2: STATE ENFORCEMENT PRACTICES FOR COMMERCIAL VEHICLE SECURITY

In the United States, large trucks and their drivers are subject to a number of types of regulation. In addition to the speed enforcement performed for all vehicles, commercial vehicles and commercial truck drivers are subject to vehicle size and weight regulations, vehicle and cargo inspections, hour-of-service regulations, and driver licensing requirements. Traditionally, the primary goals of state enforcement activity for commercial vehicles have been:

- To ensure that vehicles and their parts are safe to operate on the highway network and that loads are properly secured
- To ensure that trucks are operating within the weights and dimensions defined by federal, state, or local regulations to limit impacts on the highway infrastructure, on traffic conditions, and on the safety of other drivers
- To ensure that drivers are qualified and physically able to safely operate their vehicles.

Although state inspection activities have generally been implemented to enforce safety and size and weight regulations, many of the practices and technologies employed can also enhance highway security. Many states perform security-specific inspections including cargo screening, radiation detection, biological and chemical hazard detection, and hazardous materials tracking. Development of advanced technologies has greatly enhanced the ability of inspectors to perform these activities. Defiance or ignorance of standard truck regulations can also be an indicator of a security threat. As a result, improvements even in safety-focused inspection practices can reduce security vulnerabilities. Recent applications of advanced technologies, including automatic vehicle identification, electronic credentialing, weigh-in-motion systems, and infrared break monitoring have improved truck safety inspection and size and weight enforcement. The following section describes the operations and technologies currently employed by state authorities for commercial vehicle security.

OPERATIONS AND TECHNOLOGIES

Vehicle Inspection

In addition to required annual vehicle inspections, states perform vehicle inspections both at static weigh station locations and at remote and roadside locations using mobile inspection units. These inspections are performed to ensure proper vehicle operations, with testing particularly focused on engine and break performance. Infrared brake monitoring (IBM) systems use infrared technologies to measure the heat of tires to determine if breaks are functioning properly (*9*). While these systems cannot yet be implemented on the main lanes on highways to examine vehicles traveling at highway speeds, they are in use at inspection sites by 11 states.

Cargo Inspection

In addition to vehicle inspections, 18 of the 19 survey respondents also perform cargo inspections. Cargo inspections range from manual vehicle searches to advanced technology implementations, such as VACIS screening systems, which allow for non-intrusive screening of cargo containers. Three surveyed states also operate separate agricultural inspection facilities, and 16 perform separate HazMat inspections in addition to general cargo inspections.

Radiation detectors are widely used at land and marines ports of entry for cargo screening. These systems may vary from the large VACIS machines that can scan a 40-foot container in six seconds currently used by Customs at POEs (*10*) to small handheld devices carried by inspection officers. Forty-seven percent of survey respondents currently use radiation detectors. A variety of technologies are also commercially available to supplement manual or canine inspections for chemical or biological weapons. Currently, only four states, all of which are located on international borders, perform chemical or biological weapons detection.

Credentialing

States require carriers to file registration, permitting, and tax information. Electronic credentialing systems allow carriers to file these to states electronically, and provide an easy means of electronically retrieving relevant data for roadside inspection authorities. Several states administer electronic credentialing as part of their Commercial Vehicle Information Systems and

Networks (CVISN) architecture (*11*). Seventy-four percent of the surveyed states currently utilize electronic credentialing.

Vehicle Tracking

Global Positioning Systems (GPS) have been widely used by carriers for several years for vehicle navigation and fleet tracking. In recent years, new GPS applications for states have been developed. Several European countries have implemented systems using GPS tracking and on-board computers for monitoring travel to charge a distance-based tax for heavy vehicles. The German Toll Collect system, which has been found to have more than 99 percent accuracy in calculating vehicle mileage (*12*), has been operational since January 2005. The state of Oregon has also pilot tested a similar system for all vehicles (*13*). Geo-fencing systems use GPS tracking and on-board communications to notify carriers or authorities when a truck has deviated from an intended route or entered a restricted area. Geo-fencing technologies have been tested in the state of Washington and in the NAFTA corridor connecting Laredo, TX and Detroit, MI (*14*). These systems would be particularly useful for tracking hazardous materials shipments. FMCSA has tested GPS tracking of HazMat shipments in Alaska and Hawaii (*15*), and the California Highway Patrol has also performed tests (*7*). However, currently, only one state participating in the survey is using GPS tracking for commercial vehicle security.

Size and Weight Enforcement

Traditional methods of size and weight enforcement include static weigh stations, which require drivers to pull off of the highway into a permanent weighing facility, and portable scales, which are transported and operated by enforcement personnel at varying locations. All of the surveyed states utilize static weigh stations and portable scales for commercial vehicle weighing and inspection. Every responding state performs weighing and inspection on major interstate highways, and 18 of the 19 also do so on secondary roadways. Nine of the ten states with major marine ports of entry (POEs) perform weighing and inspections in close proximity to marine ports, and all seven land border crossing states perform enforcement activities in close proximity to land POEs.

All 19 states currently use weigh-in-motion (WIM) systems as part of their commercial vehicle enforcement program. WIM systems, which may use piezoelectric sensor, bending beam, or load cell technologies, can be used for weight enforcement at static weigh stations, as part of a weigh station bypass system, or as part of a virtual weigh station (VWS). An additional security application may also be the use of WIM data to optimize weight enforcement planning, as has been successfully demonstrated in the Montana STARS program (*16*).

Weigh station bypass systems use radio-frequency identification (RFID) transponder technologies along with WIM and height detectors for weigh station bypass. Roadside readers wirelessly query an in-vehicle transponder for vehicle identification information, which then returns credentialing and permitting data to a computer located in the weigh station's inspection station. Once height, weight, permitting, and credentialing information are verified, the computer sends a signal back to the truck, again via a roadside antenna, indicating whether or not the truck can bypass the system. Currently 13 of the 19 surveyed states (68.4 percent) are using these systems. Nine of these states (47.4 percent) participate in PrePass, the nation's largest pre-clearance system, which is operated as a public-private partnership and requires qualified carriers to apply for enrollment and to participate financially. The other four (21.1 percent) belong to Norpass, the nation's second largest system, or operate an independent state program; all of these states depend on state funding for operations and do not require a fee for participation. These sample percentages are very close to the nation-wide state participation percentages of 50 percent for PrePass (*17*) and 22 percent for state-operated systems (*18*). Although the technologies used by the PrePass and Norpass systems are identical, the systems are not completely interoperable; while PrePass transponders can be enrolled in Norpass and individual state bypass programs, carriers using non-PrePass transponders cannot bypass weigh stations in PrePass states without enrolling in the system. In Florida, AGPass enrolled carriers can also use RFID transponders to bypass agricultural interdiction facilities (*19*).

Virtual weigh stations (VWS) use roadside cameras to collect visual images of license plates or USDOT numbers and WIM systems to collect truck weight information. These systems may also use height detectors to verify legal dimensions. Data is then transmitted to roadside computers which use optical character recognition (OCR) to identify a vehicle and verify permits

and credentials. OCR-based systems have been tested in Florida, California, Kentucky, Indiana, and Saskatchewan. While many advantages to using VWS in addition to or instead of static stations, including the ability to automatically identify a vehicle without enrollment and to perform weight enforcement on secondary routes have been identified, VWS are still facing some technological barriers. Identification and installation of necessary communications systems can be difficult depending on the location of the VWS (*20*). Additionally, environmental conditions such as precipitation and light, or lack thereof, and truck characteristics, such as vehicle or USDOT number color, or USDOT number placement, can negatively impact system accuracy. VWS technologies currently available to states have not yet reached the accuracy levels that can be achieved with transponder-based identification. While three of the surveyed states have tested virtual weigh stations, only one state is currently operating an OCR-based system. Cameras employed by VWS to identify vehicles also have the potential to be used to identify stolen vehicles or vehicles traveling outside of an approved route.

SECURITY PLANNING AND INTER-AGENCY COOPERATION

Achieving a truly secure commercial highway freight transportation network requires thorough planning and cooperation of government and industry stakeholders at international, national, state, inter-state, and local levels. While existing organizations, including CVSA and the ATA, have provided forums for communications and information sharing, there is still significant opportunity for improving communications and coordination. When this survey was conducted, only 4 of the surveyed states had completed comprehensive plans for CV security, although one state has incorporated CV security planning into a broader state security plan, and one has developed a comprehensive plan for HazMat security.

Survey respondents were asked to identify with which agencies they have consulted or collaborated in CV security planning. The only agency with which a majority of states have consulted in planning for CV security was FMCSA (57.8 percent). This result is not surprising, as FMCSA is responsible for regulation of HazMat carriers, who potentially provide the greatest threat if not secured. At the federal level, a little more than one third of states have conferred with U.S. Customs and TSA, and 3 states have worked with other agencies within DHS. At the state government level, close to half of states have worked with State DHS, and more than a

quarter have worked with local authorities and other state agencies. Only 3 states have specifically collaborated with neighboring states for security planning; however, more than 40 percent have consulted with CVSA, which provides a forum for state to state communications. In at least some states, industry has played an active role in security planning, with nearly half of states having consulted with state trucking associations, more than 25 percent with national trucking associations, and 2 states even with individual carriers. However, while some states have communicated with as many as 14 agencies in CV security planning, nearly a third of states have had no inter-agency coordination. Although the sample size is not sufficient to measure statistical significance, it appears that, in general, those states located along international land borders have consulted with both government and industry at higher rates than non-border states (Figure 2).

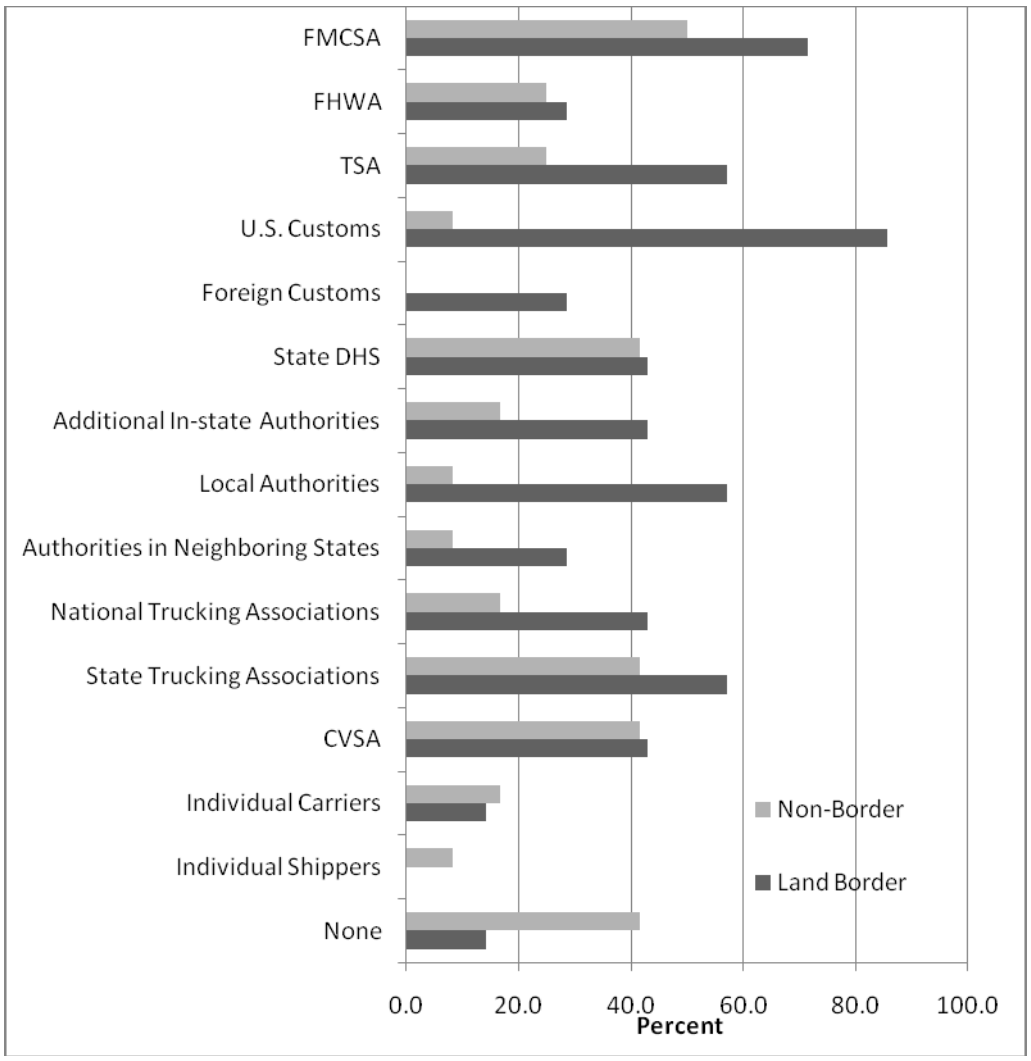

Figure 2. Inter-Agency Cooperation: Land Border vs. Non-Border States

CHAPTER 3: CHANGES SINCE 9/11

Since 9/11, focus on transportation security has increased. As a result, many operational and technological changes have been implemented (Figure 3).

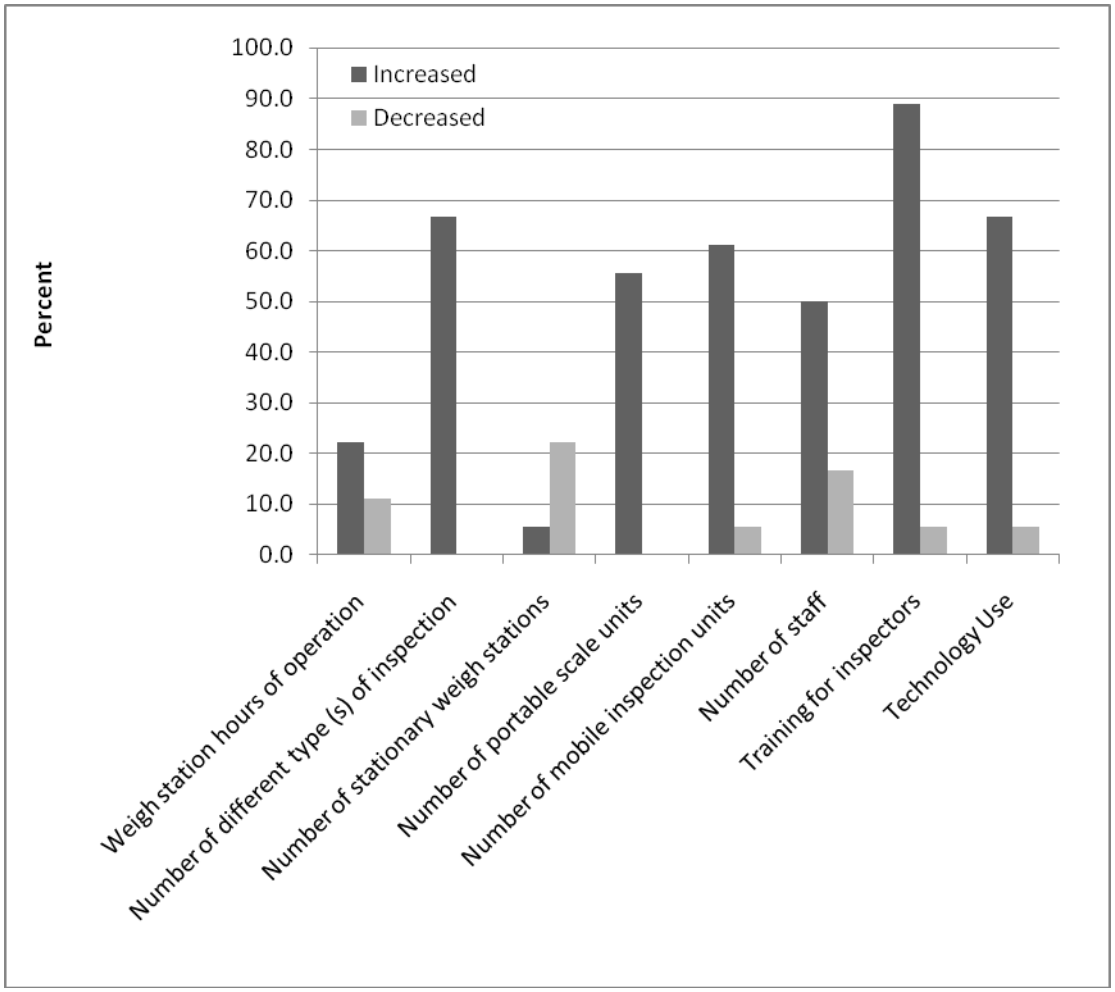

Figure 3. Operational Changes Since 9/11

OPERATIONAL CHANGES

The most widely implemented change by state authorities has been increased training for inspectors; nearly 90 percent of states have increased training requirements. This training has

focused on various aspects of security, including inspecting vehicles and cargo, identifying fraudulent identification and documents, terrorism interdiction, and incident response.

More than 60 percent of states have increased their use of mobile inspection units, and more than half have increased their number of portable scales. These provide some advantages over static weigh stations since they do not require expensive construction and may also catch violating trucks that can take secondary routes to avoid static stations. While 4 states have reduced their number of static weigh stations, only one has begun constructing a new inland facility since 9/11. In addition to expensive land acquisition and construction costs, static stations also require land availability, which may be lacking, particularly in urban areas. Three of the 4 states that have reduced their number of static stations have increased their number of portable scales and mobile inspection units.

Half of the surveyed states have increased their staff size. Several states indicated that staff was increased either to allow for increased HazMat inspections and security compliance reviews, or to increase presence at border crossings and POEs. All four states which have seen increased weigh station hours of operation since 9/11 have also increased staff. One state indicated that while hours of operation were initially increased after 9/11, a declining number of staff has contributed to a return to pre-9/11 operational hours. Both funding constraints and military deployment of highly trained personnel have contributed to declining staff in 3 states.

Seventy-eight percent of states have developed special procedures to implement during elevated terror alerts. Most of the identified procedures focused on HazMat security, including increased inspection rates, increased Safety Permit reviews, security audits of targeted carriers, and 100 percent HazMat pull-in, even of vehicles approved for weigh station bypass. General operational changes during elevated alerts included setting up checkpoints, increased and even 24/7 weigh station operations, increased and "geographically aligned" mobile patrols, and increased presence at POEs.

TECHNOLOGY USE

Two-thirds of surveyed states have added new inspection types and increased advanced technology applications. Three states, all on the border, have added chemical or biological weapons detection to enhance cargo security, and 5 states, including 3 Border States, have also added radiation detection. One state has implemented OCR-based systems at both WIM scales and fixed weigh stations which check vehicle identification information against state and national stolen vehicle databases and terrorist watchlists. Two states have added RFID bypass, which in addition to improving productivity also increases security by allowing enforcement personnel to focus on suspicious carriers. Two of the surveyed states have also tested GPS tracking for HazMat shipments.

INTER-AGENCY COOPERATION

Since 9/11, more than 70 percent of the states have increased cooperation with federal authorities concerning commercial vehicle security. In addition to generally improved communications and information sharing, several states have received funding from DHS and FMCSA for specific programs. Several states have participated in FMCSA's Security Sensitive Visits (SSV) with HazMat carriers (*21*). One respondent particularly noted that cooperation from the upper management of FMCSA has improved. States have also coordinated with the DHS-Domestic Nuclear Detection Office to improve cargo inspections, and ICE to develop programs for identifying fraudulent commercial drivers licenses.

Five of the seven surveyed land Border States have increased cooperation with CBP since 9/11. However, even among those who have improved communications, several states indicated that little to no effort was currently being made by either state or customs authorities to further enhance communications. One state indicated that the level of cooperation at border crossing facilities was highly variable depending on staff; while state authorities had found "generous outreach" from federal officials at some facilities, they had been "completely ignored" elsewhere.

Only 40 percent of states with marine POEs have increased cooperation with Customs at ports. One state has increased the number of cross-designated officers to function as both CV

enforcement and customs officers at marine POEs, and another has worked with other state agencies and customs officials to re-designate officers during elevated terror alerts. Other cooperative activities identified include officer training from Customs and assignment of commercial vehicle unit personnel to marine and air cargo routes. Two states did indicate that another state agency was responsible for interaction with ports; however, it is unclear whether these other agencies share commercial vehicle security responsibilities or focus only on port operations and security.

Cooperation between states has also increased greatly since 9/11, with more than three quarters of responding states sharing interstate borders noting improvements. Some examples include joint border inspection operations, regular or quarterly meetings between enforcement authorities in neighboring states at both headquarter and field office levels, cooperation in interstate investigations, information sharing via email and circulars, and coordination on major interstate HazMat shipments. One state also noted that inter-state information sharing through CVSA has significantly improved.

Development of the Highway Watch® program improved communications between states, and between states and carriers (*2*). Administered by ATA in cooperation with DHS, Highway Watch® provided training to and collected information on security and safety concerns from transportation professionals, including commercial truck drivers. Information on threats deemed viable was then disseminated to federal and state enforcement authorities through the Highway Information Sharing and Analysis Center (ISAC) using a top-down approach. Close to 80 percent of surveyed states noted improvements in coordination between states and carriers for CV security, and seven states particularly mentioned the Highway Watch® program. However, Highway Watch® lost its federal funding in 2008, and is currently inactive. Additional state-carrier communications improvements identified include meetings and presentations with individual carriers and trucking associations, improved cooperation on HazMat shipments, and state participation in FMCSA's SSV program. In California, the Motor Carrier Safety Assistance Program (MCSAP) visited all 5738 licensed HazMat carriers after 9/11 to share a list of best practices and verify carrier security efforts. In Kentucky, Vehicle Enforcement officers teamed with commercial carriers to use trucks for special enforcement details.

Several states have developed innovative communication tools that provide benefits for both carriers and enforcement authorities. Florida has implemented an Electronic Freight Theft Management System that collects information via internet reporting for entry into a state-wide database (*22*). This information is then transmitted via fax to relevant authorities. Information from the database can also be used to identify patterns or related incidents of freight theft. By improving information flows and reducing personnel requirements for communications, this system can achieve improvements in both speed and likelihood of recovery of stolen freight. Several states have also developed education materials to better equip both authorities and carriers for dealing with CV security issues. The California Highway Patrol operates the Commercial Industry Education Program (CIEP), which provides training seminars for commercial vehicle operators (*23*). The Michigan State Police also developed a video titled "Seven Signs of Terrorism" to educate authorities, carriers, and the general public on suspicious behaviors that may be related to terrorist activity (*24*).

CHAPTER 4: CONTINUING NEEDS AND BARRIERS TO CHANGE

FUTURE NEEDS

Operations

Respondents recognized many needs for operational changes including increased staff sizes, improved training, and increased hours of operation. Every surveyed state indicated that more staff was needed to improve CV security, including those 9 states that have already increased staff levels since 9/11. All but three states indicated that weigh station hours of operation must be increased, including three of the four states who have already increased hours of operation. Two-thirds of states recognize increased training for inspectors as a need, including 11 of the 12 states that have already added training.

Most states recognized a need for improving traditional enforcement and inspection methods. More than 60 percent of states recognized a need for more portable scales, and close to 80 percent would like to increase their number of mobile inspection units. Only increasing the number of static weigh stations and number of inspection types were recognized as needs by less than half of the responding states, and even these were considered necessary by more than 40 percent.

Technology

All but two states also indicated that technology use must be increased in the future. States were asked which technologies they would like to implement in the future if existing barriers can be overcome. Two-thirds of states not currently using RFID pre-clearance and chemical or biological weapons detection indicated that they would like to implement these in the future. Between 50 and 60 percent of non-user states would also like to implement infrared brake monitoring, electronic credentialing, and GPS tracking. About 40 percent of non-user states would also like to implement virtual weigh stations and radiation detection

Inter-agency Cooperation

Despite all of the improvements in coordination that have been achieved since 9/11, the majority of states still recognize a need for improved communications with federal and state authorities and industry. Three quarters of states recognize further need for improved communications with federal authorities, including more than 60 percent of states where improvements have already been made. Five of the six states that have not made improvements in federal-state communications also recognize a need to do so.

Sixty-three percent of states recognize a need for better communications with other states. All of the states recognizing a need for further inter-state coordination have made improvements since 9/11. Only three states that have made improvements recognize no further need. Four states have made no improvements in inter-state coordination and recognize no need to do so.

Seventy-five percent of states also recognize a need for further communications with carriers, including more than seventy percent of states who have already made improvements. Three states have made no improvements in communications with carriers, and only one of these recognizes a need to do so.

BARRIERS TO IMPLEMENTATION

A number of barriers exist that have so far prevented these needed improvements. These include financial barriers, logistical constraints, data privacy and security concerns, and technological barriers. Specific barriers examined in this survey include cost constraints, lack of available land, lack of technology infrastructure, data security, technology system security, real or perceived technology limitations, and driver privacy and carrier privacy.

Financial Constraints

With most state budgets strained, a lack of available funding is a primary barrier to improved security practices. Eighty-three percent of states indicated that funding constraints have limited operational improvements, and 78 percent have been unable to make desired technology changes due to lack of available funds. Figure 4 shows the percent of state authorities recognizing cost as

a barrier to each operational or technology improvement. Funding constraints have especially limited security improvements that require high-cost technologies. More than 60 percent of surveyed states indicated that a lack of available funding was a barrier to implementation of chemical and biological weapons inspection, and more than 40 percent recognized cost as a barrier to GPS and VWS implementation. Cost constraints have also limited improvements to some traditional operations; more than 20 percent of states indicated that costs prevented construction of desired traditional static weigh stations. However, in general, cost concerns have been less of a barrier to other traditional operations, with no more than one state identifying high costs as a barrier to increasing use of portable scales, or mobile, cargo, or HazMat inspections. Only a few states identified high cost as a barrier to WIM application and electronic credentialing.

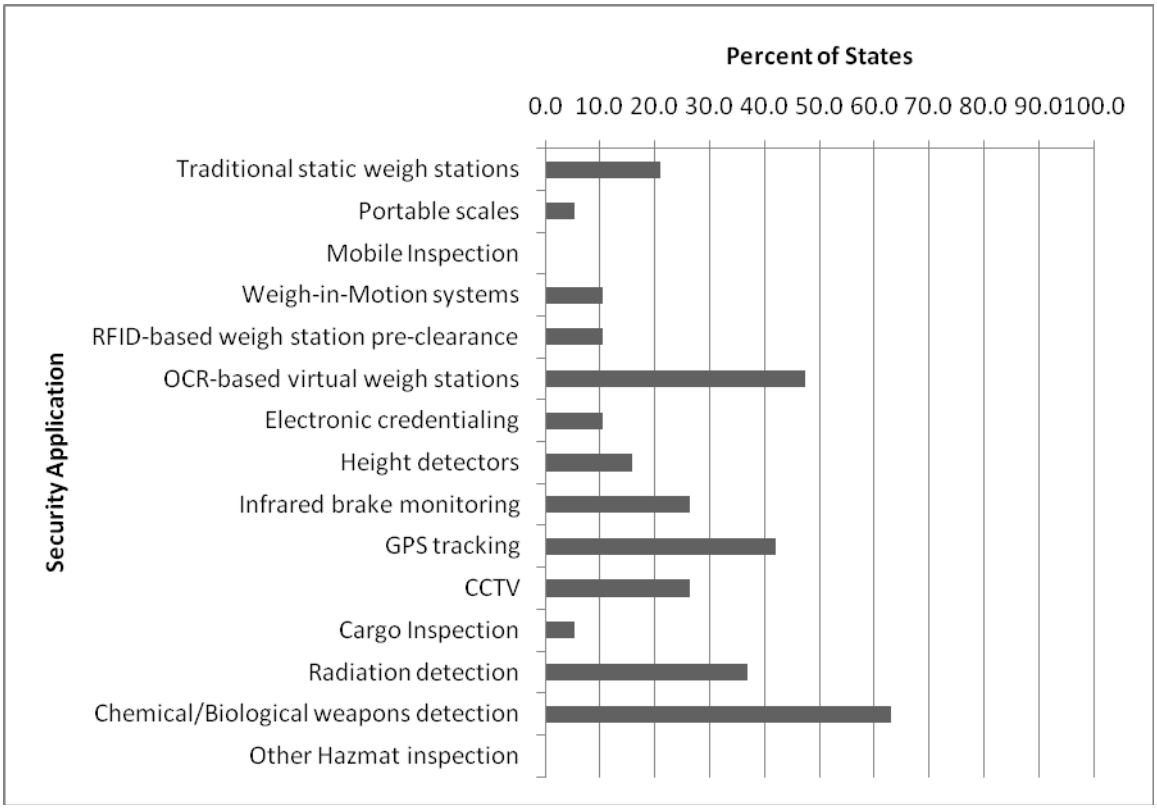

Figure 4. State Authority Recognition of Cost as a Barrier to Implementation

Logistics Constraints

A number of logistics constraints have also prevented expansion or implementation of different security operational improvements; these include a lack of space, a lack of available (or affordable) land, and a lack of power or communications infrastructure to support technology improvements. Figure 5 shows the percent of state authorities recognizing lacking infrastructure as a barrier to each operational or technology improvement. Construction of both static weigh stations and cargo inspection facilities has been limited by land availability. Implementations of advanced technologies, particularly GPS tracking and virtual weigh stations, have been limited by deficits in supporting communications infrastructure. However, only a few states identified lack of infrastructure as a barrier to WIM application and electronic credentialing.

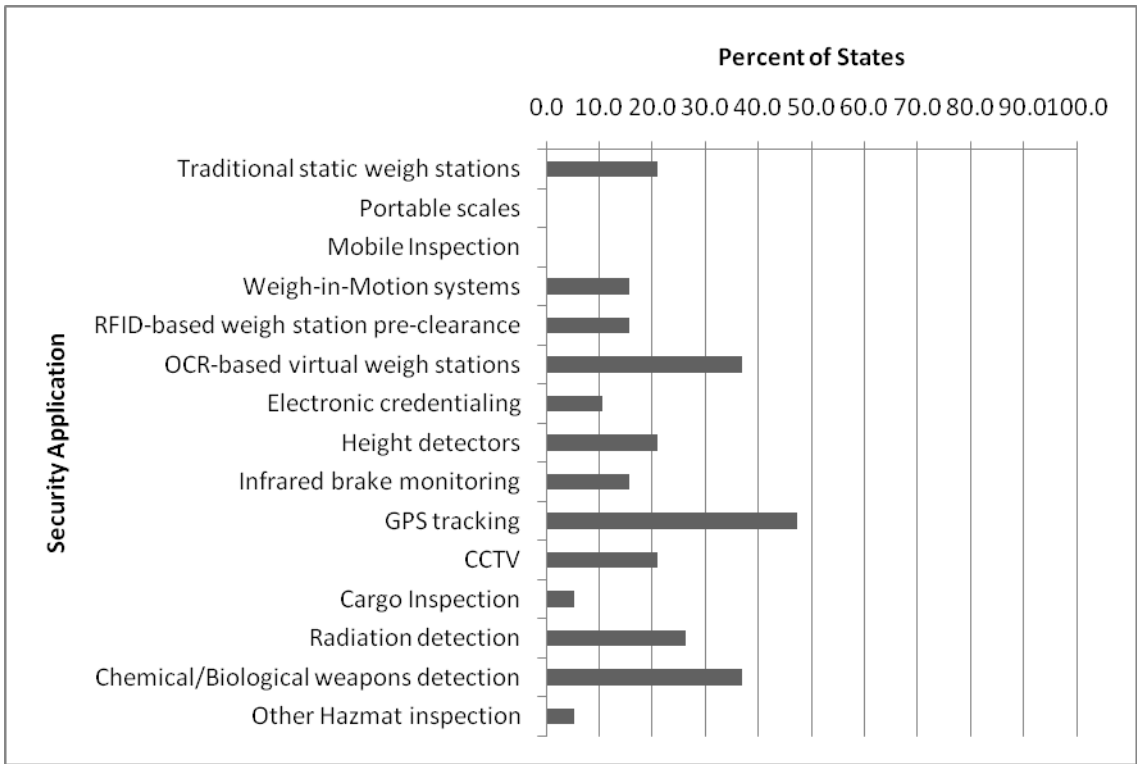

Figure 5. State Authority Recognition of Lack of Infrastructure Availability as a Barrier to Implementation

SECURITY CONCERNS

The security of both technology systems themselves and the data that they collect are definite considerations in technology implementation. Tampering with technologies can prevent or invalidate the information collected using these systems, and unauthorized access to data can expose system vulnerabilities and information about individuals and carriers (as will be discussed in Chapter 5). Security was only considered a barrier to implementation by a few states (Figure 6). OCR-based virtual weigh stations were considered sensitive to both system and data tampering by four of the 19 states. These systems are generally installed on secondary roadways, leaving them vulnerable to corruption since those tampering with cameras are less likely to be seen, particularly during low volume travel periods. GPS tracking and CCTV systems were also considered vulnerable by two state authorities. All of these systems have the potential to reveal detailed information about individuals or carriers if data security is compromised. Since GPS systems are located on-board, they are also vulnerable to tampering by the vehicle operator. One state recognized both technology and data security concerns as barriers to the use of any inspection or data collection technology except WIM and electronic credentialing, which are already widely employed.

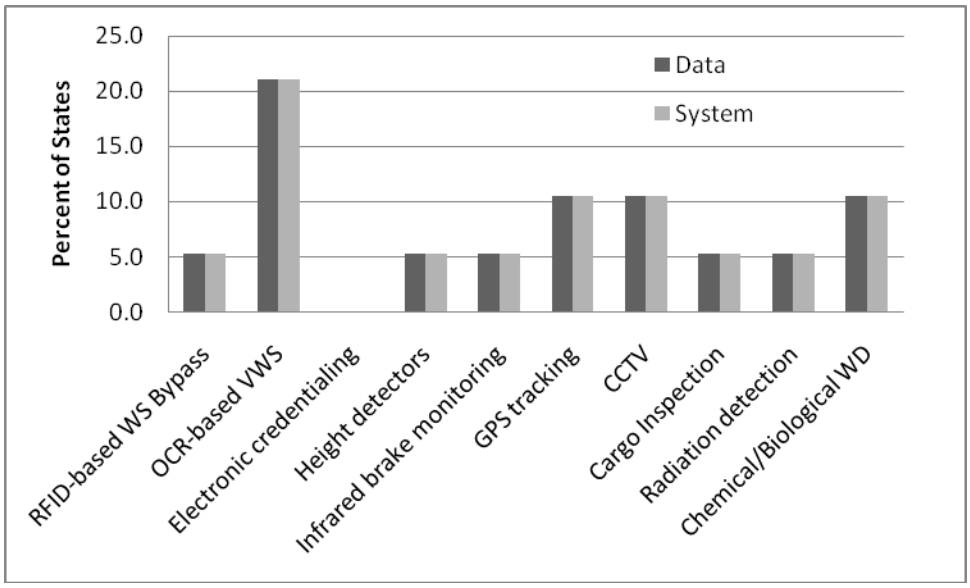

Figure 6. State Authority Recognition of Security Concerns

TECHNOLOGY CONCERNS

In order for a state to implement a new technology to improve security, the state must determine that the benefits of that technology will outweigh the costs of implementation. A number of states determined that the technologies examined in this survey would not provide security benefits (Figure 7). More than a third of the surveyed states determined that GPS would provide no security benefits, and close to a third determined than virtual weigh stations would provide no benefit. More than a quarter of states also determined that IBM and chemical/biological weapons detection would provide no benefits. Some of these results appear counterintuitive, as a number of these technologies identified as having no benefits have direct security applications in vehicle monitoring and cargo inspection. This lack of recognized benefits may result from a law enforcement perception that many available technologies have not yet been proven adequate and effective to perform their intended purpose. Figure 8 shows the percentage of state authorities that considered different technology types to be as yet unproven. As can be seen by comparing Figures 7 and 8, many of the technologies identified as providing no benefits are also considered to be unproven by a number of state authorities.

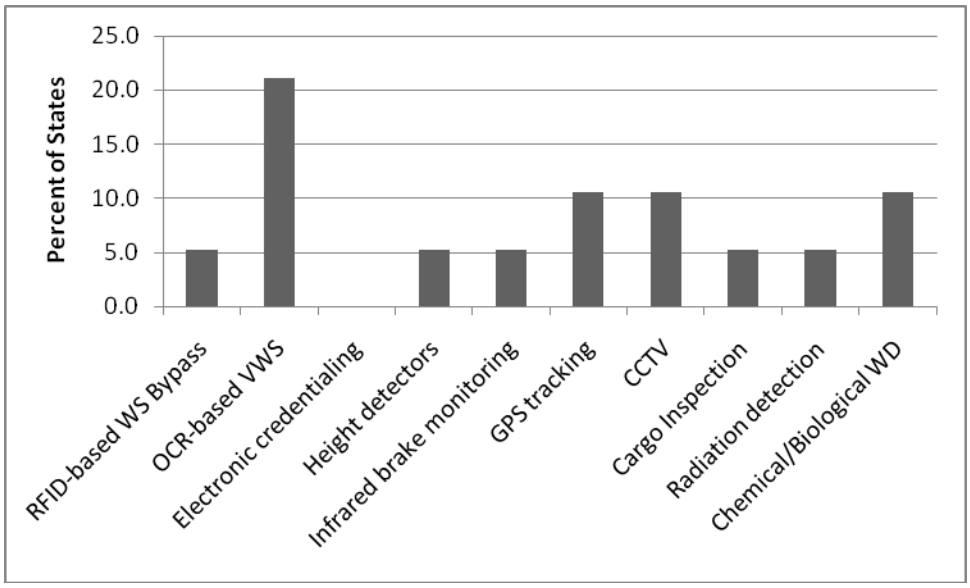

Figure 7. State Authority Recognition of No Technology Benefits

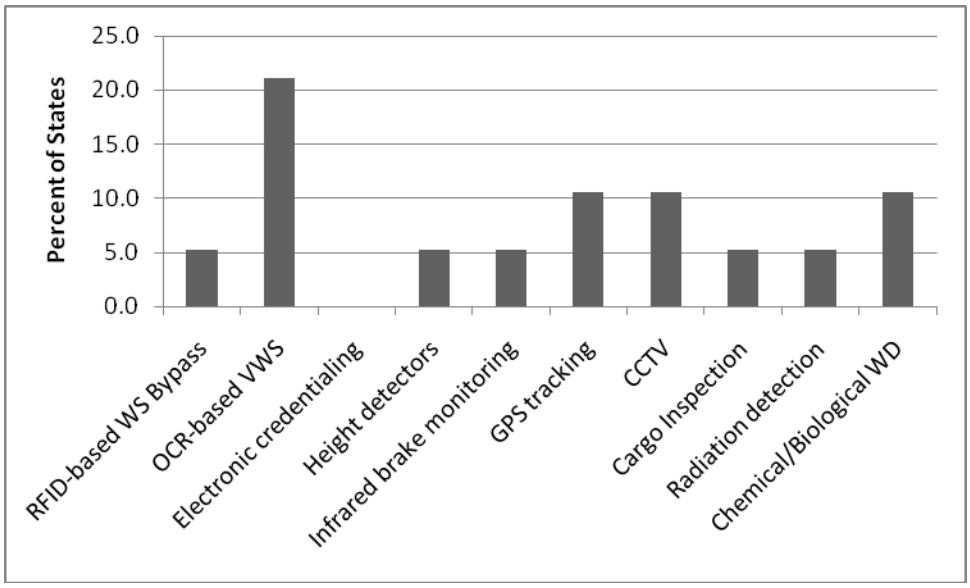

Figure 8. State Authority Recognition of Unproven Technologies

CHAPTER 5: PRIVACY VS. SECURITY

Since development of the earliest ITS technologies, privacy has been a primary user concern. Briggs and Walton identified a number of privacy related issues that arise from advanced technology implementation (*25*). The most relevant of these as potential barriers to implementing advanced technologies in commercial vehicle operations are concerns about personal privacy for a driver, concerns about company privacy for a carrier, and the potential for technology data to be utilized for secondary purposes, whether for commercial, enforcement, or illicit purposes. In addition to identifying locations and activity patterns for individual drivers, ITS data could potentially be used to track vehicle travel routes. For commercial carriers, these routes could be considered "trade secrets."

A study performed for the FHWA in 1995 comprehensively examined driver acceptance of advanced technology services; specific services examined included commercial fleet management, automated roadside safety inspection, hazardous materials incident response, onboard safety monitoring, commercial vehicle electronic clearance, and commercial vehicle administrative processes (*26*). The study identified a number of conclusions about driver acceptance of on-board ITS which can be generalized to apply to a number of technology applications. Major findings included:

- Technologies must be "useful, effective, and reliable" to gain driver acceptance.
- Drivers are more likely to favorably view technologies that they have used
- Drivers that are employed by large carriers are more likely to accept on-board technology applications than independent owner-operators
- The most frequently cited concerns for driver non-acceptance of technology were invasion of privacy by their employer and invasion of privacy by the government.

Since the 1990s, technology use by carriers has become widespread. Many trucks, particularly those belonging to large fleets, are equipped with communications devices, GPS systems for tractor and/or trailer tracking, and transponders for electronic toll collection and weigh-station

bypass. Drivers operating these vehicles have little expectation of privacy from company supervision. Although uses of data are limited due to laws and agency structures, locations and speed information could also be identified by operating authorities. Additionally, nearly all drivers carry cellular phones which could potentially be used to identify their location at a given time through cellular triangulation or GPS.

All of these technologies had to overcome privacy and data security concerns before achieving widespread acceptance. Demonstrated benefits of these systems, which include major time and costs savings and safety improvements due to reduced weaving, less stopping and better routing decisions, had to be proven to be greater than potential losses in privacy. In recent years, the prevalence of these technologies as well as the greater national focus on securing the nation and its trade corridors, have led to more widespread technology acceptance despite privacy issues. In this survey, authorities were asked whether privacy concerns were a major barrier to implementation of individual technologies. Very few states recognized privacy as a real barrier to technology implementation. GPS was the only technology generally considered to be a potential threat to privacy, and only 2 states identified it as such.

As new technology applications develop, both for commercial vehicle enforcement and for non-enforcement purposes, new opportunities may arise for secondary use of existing ITS data to improve security. ETC systems, already operational in 21 states, collect data that could potentially be used to locate a vehicle and measure speeds, hours of operations, and distances traveled. Weigh station bypass systems, currently operational in 36 states, and electronic credentialing systems could potentially provide similar data. In Europe, GPS tracking systems are used to track vehicle locations and distances traveled for collection of a distance-based heavy vehicle tax (*12*). If monitored regularly, these systems could also be used to determine vehicle speeds and hours of operation. The European Union (EU) also requires commercial trucks to operate digital tachographs with integrated Smart Cards for recording of driver and vehicle data, including driver identification information, speeds, and hours of operation (*27*).

State authorities were also asked to what secondary uses of ITS data identify are appropriate for security applications, and whether driver privacy concerns, proprietary data security concerns, or

potential for unfair enforcement standards (particularly for enrolled carriers vs. un-enrolled carriers) might prevent enforcement use of ITS data. The vast majority of potential secondary data uses were considered acceptable by responding enforcement authorities (Table 1). All of the responding authorities indicated that using any available data to locate a stolen vehicle is an acceptable secondary use of technology. The only use which was considered unacceptable by a sizable portion of respondents was tracking of vehicle mileage for charging of a weight-distance tax; this result likely reflects enforcement agency reluctance to participate in road user charging, as several respondents indicated that their agency would not be responsible for administering such a tax.

Table 1. Acceptable Secondary Data Uses

Technology Use	**Electronic Toll Collection**	**W.S. Bypass/ E.Credentialing**	**GPS**	**Smart Card**
	% States	**% States**	**% States**	**% States**
Locate a vehicle during routine operations	82.4	76.5	64.7	n/a
Locate a stolen vehicle	100.0	100.0	100.0	n/a
Monitor vehicle routes	70.6	76.5	82.4	n/a
Monitor driver speeds	82.4	82.4	82.4	76.5
Monitor driver hours of operation	70.6	88.2	88.2	82.4
Track vehicle mileage for charging of weight-distance tax	23.5	52.9	52.9	52.9

Only about one quarter of the 17 responding states recognized using weigh-station bypass and electronic credentialing or GPS technologies to monitor vehicle routes, speeds, or hours as a violation of driver privacy. Three states indicated that using any technology to locate a vehicle during routine operations is both a violation of driver privacy and unfair to enrolled carriers (if a system requires enrollment for vehicle identification). Three states also considered use of ETC and weigh station bypass data to monitor driver speeds and vehicle routes to be unfair to enrolled carriers, and use of weigh station bypass data to monitor vehicle operations to also be unfair. Smart card use for speed or hour monitoring was also considered a violation of driver privacy by three states.

CHAPTER 6: CONCLUSIONS

This report provides a comprehensive overview of truck security operations by state enforcement authorities. It is clear from the survey results that conditions vary heavily from state to state. While some states have developed comprehensive truck security plans, others have done little comprehensive planning. In some states, authorities have interacted with federal agencies, internal and neighboring state agencies, and industry stakeholders, while in other states enforcement is planned and practiced in relative isolation.

There are a broad range of operational strategies employed for commercial vehicle security. Some of these are related to other types of enforcement; unusual results identified in vehicle or size and weight inspections or hazmat tracking may indicate a security concern. Other practices are employed primarily for security operations; these include several cargo inspection types, including radiation and chemical/biological weapons detection.

Since 9/11, some improvements have been made to improve state security enforcement. Agency staff have become better trained to recognize security threats, and, where budgets allowed, staff sizes and hours of operation have increased. Many new technologies have been tested or implemented, and in general, communications between state and federal agencies and shippers and carriers have also improved.

However, improvements have been limited by a number of barriers. Most states recognize budgetary constraints as a major barrier to implementing security improvements, whether through operational changes or through facility improvements and technology implementations. Infrastructure constraints, including a lack of available space and a lack of power or communications support, have also limited facility and technology improvements. Potential for unauthorized access or system tampering was a concern to a few states in technology implementation, and some state authorities simply did not recognize real benefits for their states from implementation of advanced technologies. Both driver and carrier privacy have generally been considered major concerns in any ITS implementation for commercial trucks; however, in this study, almost no state authorities recognized these as major barriers to security

improvements. This unexpected result is likely due to 1) a changing dynamic between privacy and security in a post-9/11 environment, 2) a growing acceptance of potentially invasive technologies, such as cellular phones, and 3) state authority bias. It is likely that if carriers or drivers were surveyed, privacy concerns would be more prominently recognized.

Overall, the results of this survey indicate that many state agencies are playing an active role in security freight trucks on the highway network. A variety of existing and emerging technologies and practices have the potential to achieve improved security operations if existing barriers can be overcome. While communications have improved in recent years, better coordination between state authorities and federal and industry stakeholders will help to close loopholes in existing security practices.

REFERENCES

1. Donath, Max, Dan Murray, and Jeff Short. *Homeland Security and the Trucking Industry*. Publication CTS 05-08. Center for Transportation Studies, University of Minnesota, Minneapolis, July 2005.

2. Ripley, Amanda. "Eyes and Ears of the Nation." Time Magazine, June 27, 2004.

3. Stock, D. et al. *Hazardous Materials Safety and Security Field Operational Tests. Volume II: Evaluation Final Report Synthesis*. Federal Motor Safety Administration, U.S. Department of Transportation, Washington, D.C., November 11, 2004.

4. Wolfe, Michael. *Electronic Cargo Seals: Context, Technologies, and Marketplace.* Prepared for ITS Joint Programs Office, U.S. Department of Transportation, Washington, D.C. July 12, 2002.

5. Free and Secure Trade Program (FAST). U.S. Customs and Border Protection, Department of Homeland Security. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/fast/. Accessed July 15, 2006.

6. Border Security Overview. U. S. Customs and Border Protection, Department of Homeland Security, Washington, D.C. http://www.cbp.gov/xp/cgov/border_security/antiterror_initiatives/border_security_overview.xml. Accessed July 15, 2006.

7. *BSM Field Tests HazMat Security System for the State of California*. The Globe and Mail, Toronto, November 19, 2003. http://www.globeinvestor.com/servlet/WireFeedRedirect?cf=GlobeInvestor/config&vg=Big

AdVariableGenerator&date=20031119&archive=nlk&slug=00000737. Accessed July 30, 2006.

8. Limitations on the Issuance of Commercial Driver's Licenses with a Hazardous Materials Endorsement. U.S. Federal Register, Vol. 69, No. 160, p. 51391-51393.

9. Christiaen, Anne-Claire and Steve J. Shaffer. *Evaluation of Infrared Brake Screening Technology: Final Report.* Research Report DOT-MC-01-007. Federal Motor Carrier Safety Administration, U.S. Department of Transportation, Washington, D.C., December 2000.

10. Mobile Vacis Inspection System: Overview. SAIC. http://www.saic.com/products/security/mobile-vacis/. Accessed July 15, 2006.

11. Commercial Vehicle Information Systems and Networks (CVISN) Homepage. Federal Motor Carrier Safety Administration, U.S. Department of Transportation, Washington, D.C. http://cvisn.fmcsa.dot.gov/. Accessed July 15, 2006.

12. *Germany's High Tech Toll System Successfully Tested*. eGovernment News, European Commission, July 8, 2004. http://europa.eu.int/idabc/de/document/3151/354. Accessed July 15, 2006.

13. Office of Innovative Partnerships and Alternative Funding Road User Fee Pilot Program. Oregon Department of Transportation, 2006. http://www.oregon.gov/ODOT/HWY/OIPP/mileage.shtml. Accessed July 15, 2006.

14. Commercial Truck and Bus Safety Program Synthesis 10: Alternative Truck and Bus Inspection Strategies. Research Report CTBSSP-10. TRB, National Research Council, Washington, D.C., 2006.

15. Williams, David et al. *Expanded Satellite-Based Mobile Communications Tracking System Requirements.* Research Report FMCSA-MCRRT-06-005. Federal Motor Carrier Safety Administration, U.S. Department of Transportation, Washington, D.C., March 2006.

16. Stephens, Jerry, et al. *An Evaluation of Montana's State Truck Activities Reporting System*. Motor Carrier Services and Planning Divisions, Montana Department of Transportation, August 11, 2003.

17. National System Site Map. Affiliated Computer Services, Inc., 2006. http://www.cvo.com/map.htm. Accessed July 15, 2006.

18. NORPASS Coverage Map. NORPASS, Inc. http://www.norpass.net/coverage%20map.htm. Accessed July 15, 2006.

19. AGPASS Homepage. Affiliated Computer Services, Inc., 2006. http://www.cvo.com/map.htm. Accessed July 15, 2006.

20. Crabtree, Joseph D., David Q. Hunsucker, and Jennifer Walton. *Development, Deployment, and Evaluation of a Remote Vehicle Monitoring System and a Virtual Weigh Station*. Research Report KTC-05-38/SPR240_02_1F. Kentucky Transportation Center, University of Kentucky, Lexington, KY, November 2005.

21. *SSV Report to Congress*. Federal Motor Carrier Safety Administration, U.S. Department of Transportation, Washington, D.C. http://www.fmcsa.dot.gov/about/news/testimony/SSV-Report-To-Congress.htm. Accessed July 15, 2006.

22. Kerr, Patrick. *Evaluation of an Electronic Freight Theft Management System to Minimize Capture Time, Aid in Cargo Theft Recovery, and Improve State Economic Development – Phase III*. Research Report 548-12. Florida Department of Transportation, Tallahassee, February 2006.

23. Commercial Industry Education Program. California Highway Patrol, Sacramento, CA, 2006. http://www.chp.ca.gov/html/ciep.html. Accessed July 30, 2006.

24. *The Seven Signs of Terrorism*. Video Released by Michigan State Police, 2005. rtsp://mdch.train.org:8080/seven.rm. Accessed July 30, 2006.

25. Briggs, Valerie and C. Michael Walton. *The Implications of Privacy Issues for Intelligent Transportation Systems (ITS) Data*. Technical Report, SWUTC/00/472840-00075-1. Center for Transportation Research, Austin, TX, May 2000.

26. *Task B Final Report: User Acceptance of Commercial Vehicle Operations (CVO) Services: Critical Issues Relating To Acceptance of CVO Services by Interstate Truck and Bus Drivers*. Technical Report DTFH61-94-R-0018, Federal Highway Administration, U.S. Department of Transportation, Washington, DC, August 1995.

27. Digital Tachographs. Driving Standards Agency, Driver Vehicle Licensing Agency, Vehicle and Operator and Services Agency, and Vehicle Service Agency, Government of the United Kingdom. http://www.digitaltachograph.gov.uk/econtent/digitac/digitac.htm. Accessed July 15, 2006.

APPENDIX A: SURVEY QUESTIONS

ADVANCED TECHNOLOGY APPLICATIONS FOR COMMERCIAL VEHICLE SECURITY

STATE AUTHORITY SURVEY

Name: _____

State: _____

Agency: _____

Email: _____

Phone: _____

CV Practices and Technology Use (7 questions)

(Please circle response unless otherwise noted.)

1. Has your state completed a comprehensive plan for commercial vehicle security?

YES NO

2. Are you aware of cooperation with any of the following for development of a security plan for your state? **(Please check all that apply)**

_____ FMCSA
_____ FHWA
_____ TSA
_____ U.S. Customs
_____ Foreign Customs (Canada/Mexico)
_____ State DHS
_____ Additional authority(s) in your state (Please specify)

_____

_____ Local Authorities
_____ Authorities in neighboring states
_____ National Trucking Associations
_____ State Trucking Associations
_____ CVSA
_____ Individual carriers
_____ Individual shippers
_____ Individual receivers
_____ Other (please specify)

_____

3. Does your state perform commercial vehicle weighing and inspection at any of the following locations? **(Please check all that apply)**

_____ Major interstate highways
_____ Other major U.S. and state routes
_____ Secondary and local roadways
_____ In close proximity to marine ports
_____ At interstate land points of entry
_____ At international land points of entry
_____ Other (Please specify):

_____

4. Please describe your state's past, present, and anticipated future practices and technology use for commercial vehicle weighing, inspection, and monitoring. Were any of these specifically introduced after 9/11 to enhance security? Should your state apply any of these in the future if existing barriers to implementation can be overcome?**(Please check all that apply)**

	Prior to 9/11	Post 9/11	Introduced to enhance security?	Future Application
Vehicle Weighing				
Traditional static weigh stations				
Mobile scales				
Weigh-in-Motion systems				
RFID-based weigh station pre-clearance				
OCR-based virtual weigh stations				
Vehicle Inspection/Monitoring				
Electronic credentialing				
Height detectors				
Infrared brake monitoring				
GPS tracking				
CCTV				
Cargo Inspection				
Radiation detection				
Chemical/Biological weapons detection				
Other Hazardous material inspection				
Additional Technologies				
Other (Please specify):				

5. If your state does not utilize these inspection strategies and technologies, what are the primary barriers that prevent their application? **(Please check all that apply)**

Technology	High cost	Inadequate Infrastructure	Benefits or Effectiveness not clearly demonstrated	Unproven technology	Carrier privacy concerns	Driver privacy concerns	Data not secure from unauthorized access	System not secure from unauthorized access
Vehicle Weighing								
Traditional static weigh stations								
Mobile scales								
Weigh-in-Motion systems								
RFID-based weigh station pre-clearance								
OCR-based virtual weigh stations								
Vehicle Inspection/Monitoring								
Electronic credentialing								
Height detectors								
Infrared brake monitoring								
GPS tracking								
Cargo Inspection								
Radiation detection								
Chemical/ Biological weapons detection								

6. Are HazMat carriers currently eligible for weigh station bypass in your state?

YES NO

7. Does your state operate separate agricultural inspection facilities?

YES NO

8. Are commercial drivers licensed in your state required to participate in the Highway Watch Program?

YES NO

Changes since 9/11 (14 questions)

1. Since 9/11, has your state made any operational changes to CV inspection practices? **(Please circle all that apply and describe changes)**

Weigh station hours of operation	Increased	Decreased	No Change
Number of different type (s) of inspection	Increased	Decreased	No Change
Number of stationary weigh stations	Increased	Decreased	No Change
Number of portable scale units	Increased	Decreased	No Change
Number of mobile inspection units	Increased	Decreased	No Change
Number of staff	Increased	Decreased	No Change
Training for inspectors	Increased	Decreased	No Change
Technology Use	Increased	Decreased	No Change
Other (Please specify) _____	Increased	Decreased	No Change

Please describe changes in detail:

_____

_____

_____

_____

_____

_____

_____

2. In your opinion, could your state benefit from any operational changes? **(Please circle all that apply)**

Weigh station hours of operation	Increased	Decreased	No Change
Number of different type(s) of inspection	Increased	Decreased	No Change
Number of stationary weigh stations	Increased	Decreased	No Change
Number of portable scale units	Increased	Decreased	No Change
Number of mobile inspection units	Increased	Decreased	No Change
Number of staff	Increased	Decreased	No Change
Training for inspectors	Increased	Decreased	No Change
Technology Use	Increased	Decreased	No Change
Other (Please specify) _____	Increased	Decreased	No Change

3. Have financial constraints prevented your state from achieving desired technology improvements in security for commercial vehicles?

YES NO

4. Have financial constraints prevented your state from achieving desired operational improvements (training, hours of operations, etc.) in security for commercial vehicles?

YES NO

5. Are current federal regulations adequate to ensure reasonable security on the nation's commercial vehicle freight network?

YES NO

6. Since 9/11, has cooperation between state authorities and federal agencies increased concerning commercial vehicle security practices and requirements in your state?

YES NO

If yes, please describe improvements:

_____

_____

_____

7. Is there a recognized need for increased cooperation with federal authorities to improve the efficiency and effectiveness of commercial vehicle security in your state?

YES NO

8. If your state shares at least one international land border crossing, has cooperation with U.S. customs authorities concerning truck security at land border crossings increased since 9/11?

YES NO

If yes, please describe improvements:

_____

_____

_____

9. If your state is home to at least one major marine port of entry, has cooperation with U.S. customs authorities concerning truck security at ports increased since 9/11?

YES NO

If yes, please describe improvements:

_____

_____

_____

10. Has cooperation between yours and neighboring states increased concerning commercial vehicle security practices and requirements since 9/11?

YES NO

If yes, please describe improvements:

_____

_____

11. Is there a recognized need for increased cooperation between neighboring states and yours to improve the efficiency and effectiveness of commercial vehicle security in your state?

YES NO

12. Has cooperation between your state and carriers increased concerning commercial vehicle security practices and requirements since 9/11?

YES NO

If yes, please describe improvements:

_____

_____

13. Is there a recognized need for increased cooperation between your state and carriers to improve the efficiency and effectiveness of commercial vehicle security in your state?

YES NO

14. Does your state implement any special commercial vehicle security procedures during an elevated terror alert?

YES NO

If yes, please describe:

_____

_____

15. Has your state developed any special programs (e.g. training programs, interactions with carriers, etc.) that you think could be beneficial if applied in other states?

YES NO

If yes, please describe:

_____

_____

_____

Privacy Implications of Advanced Technology Use (2 questions)

1. Please describe your opinion on the use of advanced technologies and their data **by enforcement authorities**.

(Please check all that apply)

	is an acceptable use of technology	is a violation of expected driver privacy	may jeopardize the security of proprietary data	may unfairly hold technology users to stricter standards	may provide valuable productivity benefits for authorities	may provide valuable safety benefits	may provide valuable security benefits
Using technologies applied and data collected for electronic toll collection to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for charging of weight-distance tax (where applicable)							
Using technologies applied and data collected for electronic credentialing and weigh-station bypass to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for charging of weight-distance tax (where applicable)							
Using GPS or cellular technologies to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for charging of weight-distance tax (where applicable)							
Using Smart Cards to…							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for charging of weight-distance tax (where applicable)							

2. Please describe your opinion on the use of advanced technologies and their data **by carriers**. **(Please check all that apply)**

	is an acceptable use of technology	is a violation of expected driver privacy	may jeopardize security of proprietary data	is unacceptable for another reason (please specify)	may provide valuable productivity benefits for carriers	may provide valuable safety benefits	may provide valuable security benefits
Using technologies applied and data collected for electronic toll collection to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for payment of weight-distance tax (where applicable)							
Using technologies applied and data collected for electronic credentialing and weigh-station bypass to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for payment of weight-distance tax (where applicable)							
Using GPS or cellular technologies to…							
locate a vehicle							
monitor vehicle routes							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for payment of weight-distance tax (where applicable)							
Using Smart Cards to…							
monitor driver speeds							
monitor driver hours							
track vehicle mileage for payment of weight-distance tax (where applicable)							