CHAPTER 3

COMMERCIAL TRUCKING INDUSTRY

3.1 INTRODUCTION

Since the 1983 truck bombing of the U.S. Marine barracks in Lebanon, the United States has taken the threat of truck bombs used as weapons of terror seriously. However, not until the 1993 attack on the World Trade Center had the United States experienced a serious domestic terrorist attack committed through the use of a truck bomb. The most recent and serious truck bomb attack in the United States occurred in 1995 at the Murrah Federal Building in Oklahoma City, Oklahoma. The events of 9/11 re-ignited concerns that trucks can be used as instruments in terrorist attacks. Examples of security professional concerns include the following:

- Cargo tank trucks used as the sources and delivery vehicles of flammable (e.g., gasoline and jet fuel) and hazardous (e.g., poisonous, caustic, and radioactive) material against critical targets.
- Military cargo used as the source and delivery vehicle of explosive and radioactive material for dispersion, detonation, and blackmail.
- Cargo tank content used as source material for the production of weapons (e.g., diesel fuel and fertilizer) and as a medium for contaminating food and water resources.
- Trucks used as vehicles for the delivery of separately obtained weapons (e.g., explosives, radioactive materials and dirty bombs, and biological and chemical agents).

Although there have been both government and industry efforts to tighten security, the use of trucking industry assets to commit terrorism continues to be a perceived threat because of the large number of trucks carrying large quantities of hazardous and military cargo and the relatively high frequency of major security breaches (e.g., hijackings and other theft crimes) that occur in the commercial trucking industry. There is no centralized reporting of truck cargo thefts. The FBI estimates $12 billion to $20 billion is lost annually in truck cargo thefts, which is a fraction of a percent of the Bureau of Census estimations of approximately $4.9 trillion in annual U.S. truck cargo.[1] The ATA believes that even the higher FBI estimates are substantial underestimates.[2] This is supported by sources such as the New Jersey State Police, whose Cargo-Theft Unit estimates that only 5 to 10 percent of truck cargo theft is reported. These estimates are determined from the amount of stolen cargo found that was not reported to be stolen or lost and estimates that about $100 of the cost of a retail computer is due to the need to recoup cargo-theft loses.[3] Although a breakdown of types of cargo stolen was not found, conversations with various industry representatives suggest that theft of HAZMAT cargo is a small proportion of reported cargo thefts. Reporting of HAZMAT thefts are difficult to avoid as a result of U.S. DOT tracking required for the shipment of hazardous materials. However, theft of nonhazardous cargo may also be of concern from the standpoint of use in terrorist acts; an example of this was the truck theft last May that included a shipment of airline employee uniforms.[4] Thus, the magnitude of cargo theft, regardless of whether the cargo is hazardous, suggests the validity of truck cargo-theft concerns.

The development of centralized cargo-theft reporting may assist in future assessments of cargo-theft risks and could be an important role for either the government or national organizations. However, centralized reporting may not reduce underreporting of thefts if the reason for underreporting is to keep insurance rates low, as has been suggested by industry experts.

Unfortunately, even if the commercial trucking industry were perfectly secure and inaccessible to terrorists, the means and the opportunity for executing a terrorist act involving trucks would not be eliminated and perhaps not even reduced. This is due to the ready access to trucks through truck rental agencies (short-term), leasing organizations (long-term), new and used truck dealerships, private sellers, importers, and theft rings—all of which may do business through the Internet. Access to many hazardous materials can be obtained legally (e.g., diesel, gasoline, fertilizers, and other base chemicals used

[1] Includes both commercial trucks for hire and trucks owned by either the sender or receiver. Trucks for hire transported $2.9 trillion worth of cargo in 1997. *1997 Commodity Flow Survey,* Bureau of Census, Table 1a.

[2] Jeanne Strong, Director Claims, Safety & Loss Prevention Management Council, American Trucking Associations, Alexandria, VA.

[3] "Sneaker Thefts Part of a Trend, Cargo Heists Often Go Unreported," *Kansas City Star,* March 15, 2003, p. A1.

[4] "Little Danger Seen in Uniform Theft," *Kansas City Star,* May 16, 2002, p. 14G.

to create poisonous and caustic substances). The purchase of these materials can also often be arranged through the Internet.

The operational characteristics of terrorists suspected of targeting U.S.-based assets include a focus on executing severe, but infrequent, terrorist acts that have maximum terror and damage impact. Time is not a factor. A patient operational approach allows time for the implementation of activities that enhance the ability of terrorists to acquire weapons, materials to make weapons, and the means to deliver them (e.g., by trucks). These activities include the following:

- Development of businesses with the appearance of legitimacy that have been established for the acquisition of vehicles and material;
- Accumulation of equipment and material for apparently legitimate uses or in small quantities, which is unlikely to arouse suspicion; and
- Development of trust and contacts with shippers and suppliers and acquisition of permits, licenses, and other administrative necessities.

In fact, most recent terrorist acts involving trucks or automobiles used legitimate means to acquire the vehicles. Both major terrorist acts in the United States using trucks (i.e., the 1993 World Trade Center bombing in New York City and the 1995 bombing of the Murrah Federal Building in Oklahoma City) used legally acquired trucks and materials to make explosives. The only known exception to the legal acquisition of trucks for carrying out terrorist acts against the United States is the truck used in the U.S. Marine barracks bombing in Lebanon (1983). In general, obtaining trucks and material illegitimately risks prematurely exposing terrorist plans and operatives; therefore, terrorists are likely to avoid this pathway.

The combination of uncertain risks of a threat, questionable effectiveness of anti-theft security measures, tight operating margins, and competition means few trucking companies are likely to internalize potential external (noncompany) losses such as the destruction of a building, tunnel, or pipeline through terrorism. With this as a background, it is easier to understand the trucking industry's perception of national-level threats, security action taken and planned, and the direction of desired research. The remainder of this chapter examines these perceptions as well as industry attitudes, past and planned actions, and the needs and opinions of the commercial trucking survey respondents.

3.2 ANALYSES

Survey responses were received from 20 trucking companies. These respondents report the following overlapping functions:

- 12 are engaged in the transport of general freight,
- 6 are tank carriers,
- 5 transport HAZMAT,
- 3 transport food grade liquid transport,
- 2 are engaged in military freight, and
- 2 are listed as dry bulk tank operators.

Several companies were described to have multiple, unspecified product/service capabilities. Only five organizations (two general cargo, two food liquid carriers, and one HAZMAT carrier) describe themselves as single-product category trucking companies. The remaining companies listed two or more product categories (e.g., HAZMAT and general cargo). Of the 20, 10 are identified as LTL carriers, 8 are Truck Load (TL) carriers, and 2 are both. Because of the many overlaps in services provided and products shipped, it is not practical to make a distinction between groups of carriers based on this survey.

The issues addressed by the 16 survey questions are grouped into the 8 issue areas listed in the scope of this report (Section 2.3). Analysis of each issue area begins with a restatement of the issue and statement of the relevant survey question(s). Summaries of the answers are tabulated and presented in detailed summary tables that provide the reader with an opportunity to delve into the specific responses of the respondents and to formulate independent observations and analyses.

Commonly, each question received one response. However, in many cases, a respondent provided multiple answers to the same question. Because of the varied number of responses per question, the tabulated responses for each question do not equal the number of respondents to the survey (20).

3.2.1 Identification of the Key Threats to the Commercial Trucking Industry

The commercial trucking industry perception of key terrorist threats to its industry was evaluated based on survey responses to the question: *What do you perceive to be the key national security (terrorism-related security) threats to your commercial trucking operations, and why?* These responses are summarized in Table 3-1.

The respondents perceive a broad set of possible threats. Their vision of the threat is not uniform, although the main threat theme involves stolen trucks for use as instruments in carrying out terrorist acts. A variation of this scenario is either expressed or implied by most respondents. The respondents also indicate a concern that the cargo, including food, weapons, explosives, nuclear material, and so forth, could be used for a terrorist attack. Others indicate that the threats are of a somewhat less direct nature such as unknowingly transporting illicit cargo and using criminal means (e.g., vandalism) to support terrorist groups. Still other responses point to events that are less related to defining the threat and more related to defining the consequences and concerns. These include concerns for the safety of drivers and customers and concerns for loss of property. Two respondents did not perceive a terrorist threat to the commercial trucking industry.

TABLE 3-1 Perceived threats to trucking operations

Perceived Threats to Trucking Operations	Number of Respondents	Percent of Total
Stealing vehicles to be used as instruments of terrorism.	7	37%
Introduction of narcotics, weapons of mass destruction, contamination of water/foodstuffs; misdelivery of dangerous goods aimed at a disastrous result; truck entry to a consignor/consignee facility with intent to do harm.	6	32%
Hijacking of trucks and drivers.	5	26%
Theft of cargo and equipment – "economic terrorism" to support special interests at our expense.	5	26%
Theft of conventional arms, ammunition, and explosives.	4	21%
Vandalism.	4	21%
Harm to employees, drivers' security and safety traveling over roads.	5	27%
Disruption of services, highways, and roadways.	2	11%
None.	2	11%
Not knowing the client and the cargo shipped.	2	11%
Organized crime and local gang elements.	2	11%
Theft of nuclear weapons materials.	1	5%

These perceptions of threats are expressed in general terms and are similar to events that have occurred elsewhere (e.g., stolen truck, Beirut, Lebanon, 1983) or are commonly voiced concerns of the security community (e.g., transporting and employing weapons of mass destruction and food/water contamination). Few specific hazards (e.g., explosions and chemical contamination) or targets are listed. The operations involved in executing the listed threats are the same initiating events used in the very common, and arguably unstoppable, cargo crimes committed daily on U.S. highways.

3.2.2 Identification of Risk Management Techniques Available to Assess Potential Security Threats

Risk management techniques used by the industry were assessed by survey responses to the following two questions: *(1) What process do you use to determine your risk exposure? (2) What risk management techniques (probabilistic risk assessment tools, vulnerability assessments, cost/benefit models, etc.) are available to you to assess potential security threats?* Responses to these questions are provided in Table 3-2 and Table 3-3.

Responses to the survey question on determination of risk exposure suggest that the industry commonly engages in assessments of threats by location (see Table 3-2). Other factors that are sometimes considered include the product, customer, crime index, run reports, and claims history/insurance statistics. These assessments are targeted more toward cargo theft than terrorist acts. However, as noted above, there is a perceived commonality and connectivity between a terrorist act and cargo theft in the mode of operation (i.e., penetrating vehicle and cargo security).

The variety of answers to the risk management question (see Table 3-3) suggests that the processes used for determining risk management are quite varied and general. Listed risk management techniques included evaluations of audits

TABLE 3-2 Process used to determine trucking operations risk exposure

Process Used to Determine Risk Exposure	Number of Respondents	Percent of Total
Threat assessments by location; implement improvements via internal/external security audits; University of Pennsylvania Crime Index for statistics to locate safe areas for truck/trailer facilities.	13	68%
Evaluate—needs vary by customer and product; Review products (dry bulk, liquid, hazardous); application information and motor vehicle record (MVR) check.	7	37%
Terminals audited for security risk exposure and accessibility.	4	21%
Operator review; facility review; customer review.	3	16%
Run reports.	2	11%
Claims history on high-value cargo; review monthly company insurance loss.	2	11%
In-transit security assessment.	1	5%
None.	1	5%
One company standard, enhanced security at high-risk locations.	1	5%

TABLE 3-3 Risk management techniques used for trucking industry threats

Available Risk Management Techniques	Number of Respondents	Percent of Total
None used.	5	26%
Security audits/facility audits; receive daily cargo theft lists.	4	21%
Company complies with military requirements.	3	16%
Use the CAP Index for local assessments; use models to evaluate costs/potential solutions and payback.	3	16%
Review American Chemical Council safety recommendations.	2	11%
Review National Tank Truck Carriers advisements (publications).	2	11%
Terminals audited for security risk exposure and accessibility.	1	5%
Due diligence on prospective customers.	1	5%
In-transit security assessment.	1	5%
Use own legal dept. to assess/evaluate safety/security needs.	1	5%
Observation and transportation groups.	1	5%
Our insurance carrier can provide help as needed.	1	5%
Review national security organizations.	1	5%
Plan ahead for stay-overs, stops, etc.	1	5%
Work with law enforcement liaison information.	1	5%

and cost/payback models in addition to due-diligence and security assessments. Some companies consider information from organizations such as the NTTC, industry publications, cargo-theft lists, insurance carriers, and law enforcement organizations in their risk management. However, the responses to the survey suggest that a significant proportion of the industry does not use or recognize the availability of more formal risk management techniques.

The many regulations and recommendations that address commercial trucking may reduce trucking company concerns about independently assessing their risk management strategies. Both risk exposure and risk management are at the root of the trucking regulations and standards that have been in place for many years to address both safety and security issues. Regulations are issued by U.S. DOT, in addition to some more rigorous state and local regulations. Specific regulations and recommendations vary by operation, cargo type, and industry group (e.g., LTL, HAZMAT, and military cargo) and are particularly extensive for HAZMAT and military cargo carriers. Hazardous materials transport regulations are issued by both the U.S. Environmental Protection Agency (EPA) and U.S. DOT for specifically designated hazardous materials, whereas the U.S. Department of Defense (DoD) regulates military cargo transport. Guidelines and recommendations are also provided by industry and private groups (e.g., the American Chemical Association), particularly for the handling and transport of hazardous bulk materials and chemicals.

Regulations and recommendations typically address technical requirements (e.g., container design and construction requirements, inspections, and maintenance); operational requirements (e.g., driving, stopping, and parking); and reporting and administrative requirements (e.g., licensing, registration, and notification). These are often based on both theoretical considerations and historical experience. However, these pre-9/11 regulations and standards only marginally address post-9/11 terrorist concerns. In response to 9/11, revisions were made to the military requirements,[5] and changes in U.S. DOT rules for the transport of hazardous material have been proposed.[6] From the answers provided to the risk exposure and management questions (Tables 3-2 and 3-3), it is not clear that trucking companies found it necessary to review and enhance existing risk exposure and management procedures as a result of 9/11. However, other parts of the survey (see Section 3.2.4) indicate that some reassessment and tightening of procedures did occur in addition to the requisite meeting of new regulations as they come into effect.

None of the respondents indicated that they used free risk assessment tools available through the government and the Internet.[7] A review of some of these assessment tools indicates that they are targeted to cargo theft. The ATA is conducting a risk assessment survey that encourages the industry to engage in a formal process to assess its exposure to terrorist acts; however, none of the survey respondents noted this activity. Standard assessment techniques that are available, but were not specified by respondents, include the following:

- **Threat Assessment,** which defines and characterizes the terrorist threat posed to the organization;
- **Risk Analysis,** which determines the likelihood of the threat occurring by location (e.g., place and activity);
- **Vulnerability Assessment,** which determines how susceptible the organization is to the threat and the points of vulnerability;
- **Effectiveness Assessment,** which tests the effectiveness of existing measures against threats and makes adjustments to fill the gaps; and
- **Cost/Benefit Analyses,** which determine what mitigation measures are prudent in terms of effectiveness, cost, and benefit.

3.2.3 Identification of Employee/Driver Hiring Procedures, Including Employee Identification/Verification Techniques, That Can Enhance Security and That Have Been Shown to Be Effective

Employee hiring and identification/verification procedures were assessed through survey answers to the following questions: *Have you revised your employee/driver hiring procedures and employee identification and verification techniques? (a) What are they now? (b) How will these be effective? (c) What other steps would help?* Responses to these questions are summarized in Table 3-4.

Trucking company hiring procedures are not standardized, but they typically include background checks (e.g., work history, criminal and reference checks, citizenship status, and financial review), and they sometimes include behavioral tests. The combination of measures used is strongly influenced by the type of service provided by the organization (e.g., HAZMAT, valuable goods shipments, and shipment of explosives). Some sectors of the industry have to meet minimum standards of due diligence in hiring. Both independent information and survey responses indicate that although some companies have significantly revised their hiring procedures, a significant proportion of the industry has not revised hiring or identification procedures since 9/11. The most common changes since 9/11 have been more thorough background checks and the use of identification cards.

With respect to ID procedures, both survey responses and independent sources suggest the use of photo IDs is increasing. Most major chemical transporters have implemented company security identification systems.[8] FMCSA Security

[5] *Defense Transportation Regulation (DTR) DoD Regulation 4500.9-R-Part II Cargo Movement,* Ch. 205; updated April 2002; www.transcom.mil/J4/j4lt/dtr.html.

[6] *Federal Register*, July 16, 2002, Vol. 67, No. 136, pp. 46622–46624.

[7] For example: "Chemical Facility Vulnerability Assessment Methodology," U.S. Department of Justice, June 2002.

[8] "Statement of Joseph M. Clapp, Administrator, Federal Motor Carrier Safety Administration, Before the House Committee on Appropriations Subcommittee on Transportation," February 13, 2002 (testimony). www.fmcsa.dot.gov/Aboutus/testimonies/2_13_02Clapp_Testimony.htm

TABLE 3-4 Revised trucking industry employee/driver hiring and identification procedures

Revised Hiring Practices/Verification Techniques	Number of Respondents	Percent of Total
No – they are safe and appropriate.	8	42%
Yes.	7	37%
Greater emphasis on background screening.	2	11%
Identification procedure changed to photo ID badges.	2	11%
Remains focused on hiring the best candidates possible.	2	11%
What are they now?		
Stricter background checks including country of birth and visited; Application verified, background and reference check, previous employment and residences.	17	64%
Mandatory criminal record checks.	8	42%
Take copies of candidate's commercial driver's license (CDL) and Social Security Card.	5	26%
Complies with U.S. DOT compliance checks for driver's prior CDL records, past employment, drug testing, and review.	4	21%
Applicants checked for felony convictions in last 10 years.	3	16%
Company complies with military requirements	3	16%
Checked for misdemeanor convictions re: breach of trust, violence, possession/distribution of drugs in last 10 years.	2	11%
Full 10-year employment history check.	2	11%
3 years + verifiable experience with a U.S.-based carrier.	1	5%
All employees get an internal ID; change in I-9 forms.	1	5%
Do behavior testing.	1	5%
How will these be effective?		
Identify potential problem candidates and disqualify them.	2	11%
Always under review for improvements.	1	5%
ID cards, Time/Attendance, Access Control, and other verification devices.	1	5%
More vigorous verification of past employment & gaps.	1	5%
U.S. DOT went through records to identify any areas of concern (there were none).	1	5%
Re-evaluated driver pool; U.S. DOT had no problems with personnel.	1	5%
What other steps would help?		
Access to National Crime Information Center (NCIC) criminal records database.	5	26%
We need a federal database/national identification system.	5	26%
Revamp the state CDL programs.	3	16%
Online security system.	1	5%
Serious Homeland Security action against "economic terrorism" (theft).	1	5%
Tax credits/relief for cost of security implementation.	1	5%

Sensitivity Visits, implemented in response to 9/11 as a means to discuss security enhancement, target carriers transporting hazardous materials in quantities that could pose a significant threat, companies that train drivers, companies that lease trucks and drivers, and high-risk facilities (e.g., chemical plants and refineries).[9] The Security Sensitivity Visits include discussion of the importance of tamper-proof photo IDs with telephone numbers for further verification.

Plans are also underway for development of a transportation worker ID card (TWIC) to be issued by U.S. DOT, with development assistance by TSA. The goal of the TWIC credentialing program is to provide a uniform, nationwide standard for secure identification of workers across all transportation modes, including the trucking industry. The TWIC will likely use SmartCard technology, including biometrics. At this stage of TWIC development, technology and common credentials for all TWIC workers are being assessed.[10]

With respect to changes in hiring practices since 9/11, discussions with operators (some of which were not part of the formal survey) indicate that even hiring practices that have remained unchanged are taken much more seriously by the hiring organizations, regulatory agencies (e.g., DoD and U.S. DOT), investigating agencies (e.g., the FBI and private security organizations), and the applicants. Since the events of 9/11, many trucking companies have "more seriously" reexamined all employee files, including those of their senior employees, and have taken personnel actions, including dismissals. The survey respondents do not provide details on how their background checks have been enhanced. However, more rigorous background considerations may be similar to those discussed in FMCSA Security Sensitivity Visits. Security Sensitivity Visit discussion points on background checks do not include specific criteria, but do include consideration of gaps in employment, frequency of job shifts, all names used by the applicant, type of military discharge, citizenship, present and prior resident information, personal references, and criminal history.

As part of the USA PATRIOT Act of 2001, Section 1012, FMCSA, in coordination with the U.S. Department of Justice, the U.S. Department of Health and Human Services, and the American Association of Motor Vehicle Administrators, is developing a security review process for hazardous materials commercial driver's licenses (CDL). States will submit requests for background investigations to the Department of Justice before licensing an individual to haul hazardous materials. Based on the results of the background records check, U.S. DOT will make a security risk determination and notify the requesting state of the result. FMCSA expects to issue an interim final rule to implement this process in the near future.

As noted in some survey responses and by other industry sources, security would be enhanced by the development of a national, standardized, reporting and information database for trucking industry personnel. This would make the investigation process more accurate and uniform, with easier information access. Currently, processing new hires is both costly and time consuming. Access to the needed information/records is constrained by state boundaries, privacy laws, loopholes, and union and employment rules. Further, concerns have been expressed regarding the reliability of some information sources. Presumably, these issues are more relevant

[9] Report on FMCSA's Security Sensitivity Visits to the House and Senate Committees on Appropriations, January 31, 2002 (an appendix of "The American Trucking Industry's Anti-terrorism Action Plan," American Trucking Associations, May 2002). This report, without security talking points, is also reproduced at: http://www.fmcsa.dot.gov/Aboutus/testimonies/SSV_Report_To_Congress.htm.

[10] Further information on TWIC status can be obtained from www.tsa.gov/public/display?content=364.

for assessing criminal history and references other than driving records. The Commercial Motor Vehicle Safety Act of 1986 established minimum national standards that states must meet when licensing commercial motor vehicle (CMV) drivers. This act makes it illegal to hold more than one license and requires that states be connected to the Commercial Driver's License Information System (CDLIS) and the National Driver Register (NDR) to exchange information about CMV drivers, traffic convictions, and disqualifications. Employing motor carriers also have access to the CDLIS; however, not all states have been in compliance with the FMCSA regulations on CMV drivers and information exchange. It is not clear if the calls by survey respondents for a national driver's license system were based on difficulty accessing or using the CDLIS, inconsistent reporting within CDLIS, or other issues. FMCSA has recently improved regulations for CMV driver data exchange and can withhold all Motor Carrier Safety Assistance Program grant funds from states that are not in compliance.[11] FMCSA is also working with the states to eliminate practices that make systems vulnerable to fraud. As these new FMCSA regulations and activities take effect, calls for a national driver's license system may subside.

To address background information other than driving records, the ATA ATAP includes improving industry access to information databases for security and criminal background checks of commercial truck drivers and possibly for other employees in sensitive positions. The great diversity in industry hiring procedures suggests that some form of regulations, standards, or guidelines regarding hiring (beyond minimum driver's license requirements) and employee identification procedures may be beneficial. The ongoing FMCSA activities (i.e., Security Sensitivity Visits and background checks for CDLs of hazardous materials drivers) concentrate on specific segments of the industry thought to represent greater terrorism-related risks, and, thus, these activities do not provide nonhazardous carriers with guidance on hiring and identification security improvements.

3.2.4 Identification of Current Security Procedures at Commercial Truck Training Schools and Potential Threats, Including Student Identification/Verification Procedures

Information on security procedures and potential threats at training schools was gathered from interviews with training schools and from the following question presented to trucking company survey respondents: *Do you use training schools? If yes, what security procedures are employed at commercial training schools for your industry (e.g., student identification/verification procedures), and do you consider these to be effective?* Trucking company responses to this question are presented in Table 3-5.

TABLE 3-5 Trucking industry use of training schools and level of effectiveness

Use of Training Schools and Level of Effectiveness	Number of Respondents	Percent of Total
Do not use them; our drivers need minimum of 1–3 years experience.	7	37%
Not applicable/unknown.	6	32%
We provide additional in-house training.	2	11%
We won't hire someone just out of school to haul liquids.	1	5%
Candidates must go through in-house security training.	1	5%
We understand a competitor has a very good driving school.	1	5%

The responses in Table 3-5 suggest that most of the trucking companies surveyed either do not hire drivers directly from training schools, or their in-house hiring and training practices negate the relevance of what is done in training schools. The companies represented in this survey are generally larger than the average company in the trucking industry; therefore, the relevance of training school curriculum and student verification procedures may be greater for smaller trucking companies.

Several training schools were contacted to inquire about their security-related curriculum and admissions requirements. Prior to 9/11, training schools had criteria for accepting students that included eligibility requirements (e.g., active driver's license and U.S. citizenship or green card), general performance requirements (e.g., ability to read English), and some security requirements (e.g., must wear ID while on premises and must be fingerprinted). Those without a green card or work permit papers were not admitted. However, the overall focus was on safety and theft issues.

After 9/11, schools became more concerned about admittance of foreign students and improving security at their facilities. Efforts were made to obtain terrorist-related information. Regarding student acceptance practices, respondents noted that there were no significant changes in their acceptance criteria and that they have no specific practices to assess criminal or terrorist intent. Some of the reasons or impediments provided for not focusing on security, specifically terrorist-related security, were cost, area of the country does not seem to be a target, the training institution is a public organization and has limits on soliciting personal information, clients do not see a focus on security as a requirement, and students note that any focus on security is "an overkill."

The training curriculum was reported by one respondent to have been changed slightly since 9/11 to include familiarity training with theft deterrence devices. Another respondent reported the willingness to include security information in their training curriculum, but noted that clients do not call for this type of knowledge. Several schools in states that are part of the ATA HWP mentioned they didn't currently see a need

[11] *Federal Register,* July 31, 2002, Vol. 67, No. 147, pp. 49741–49764.

for awareness training as part of their curriculum because free awareness training is provided by their state trucking association in conjunction with the state highway patrol.[12] In general, training schools respond to industry needs; therefore, more rigorous student admission requirements and further expansion of curricula to include security issues may not occur until the minimum industry hiring and security training requirements are more uniformly rigorous.

3.2.5 Identification of Security Procedures and How Technology Can or Is Being Used to Address Security Issues

Survey questions were designed to gather information on trucking company security procedures in three time frames: pre-9/11, current (post-9/11), and in the near future. The following question addressed pre-9/11 security procedures at trucking companies: *What national security measures were in place prior to 9/11 to address what threat? If None: Why?* Responses to this question are presented in Table 3-6.

Current (post-9/11) trucking company security procedures were addressed by the following three survey questions: (*1) What national security measures did your organization take following 9/11 regarding: employees, customers, public, cargo transport, hazardous material, other? If None: Why? (2) What national security measures were instituted by your shippers and consignees after 9/11, and how do these measures impact security and your operations? (3) Can you summarize what other members of your industry are doing?* Responses to these questions are presented in Tables 3-7, 3-8, and 3-9.

Near-future changes in trucking company security procedures were assessed by the following survey question: *What additional national (anti-terrorism) security measures are planned for this year? Over the next several years? If None: Why?* Responses to these questions are presented in Table 3-10.

The use of specific security technology in the commercial trucking industry was assessed by the following survey question: *What technologies are you employing to address security issues? If None, Why?* Responses to this question are presented in Table 3-11.

Prior to the events of 9/11, the trucking industry did not design its security program to protect against a terrorist threat. Yet, because of the strict HAZMAT shipping regulations, the even more austere military shipping regulations, and the general industry effort to minimize cargo theft, many of the pre-9/11 security measures were similar in function (if not intent) to anti-terrorist measures. Pre-9/11 security measures are summarized by survey responses presented in Table 3-6.

TABLE 3-6 Pre-9/11 trucking industry security measures

Security Measures in Place Prior to 9/11	Number of Respondents	Percent of Total
Better sealing systems for tank trailers.	6	32%
We are very careful of what we did before; 9/11 caused us to re-evaluate then follow company policy.	6	32%
Higher scrutiny for driver background checks.	5	26%
Use of padlocks and trailer seals; very tight seal control policies.	5	26%
Company complied with military requirements pertaining to physical security program.	3	16%
Enhanced terminal security; guard security.	3	16%
Increased training programs for drivers; heightened awareness during weekends and holidays.	3	16%
None.	3	16%
Enhanced automated technology, electric fences, cameras, and access controls.	2	11%
HAZMAT training and customer identification.	2	11%
No locked tankers to be left unattended.	2	11%
Various mandated U.S. DOT requirements for safe handling of HAZMAT cargos.	2	11%
Economic terrorism overlooked by federal law enforcement agencies; we've enhanced focus on security-related issues reflected in item #3; our theft deterrence actions work well with Homeland Security initiatives.	1	5%
Restriction of prior commodities and wash facilities.	1	5%
Utilization of satellite tracking communications.	1	5%
If None: Why?		
There was no issue to address other than loss prevention.	2	11%
Big emphasis on employee screening, employee/terminal security; sealed loads; use of padlocks/trailer seals.	1	5%

Trucking industry security measures prior to 9/11 included both physical measures (e.g., locking and sealing devices, terminal security, cameras, and other security devices), and policies and practices applicable to protecting against terrorist acts. The latter include stricter background checks, increased training, and more rigorous compliance with HAZMAT regulations.

The security measures implemented after 9/11 reflect changes in the perception of terrorist threats and reveal a realignment of trucking company security concerns. The large number of changes indicates that pre-9/11 measures were broadly inadequate in addressing the newly perceived risks. The most common post-9/11 changes were establishment of an anti-terrorism policy, awareness/security training, and issuance of IDs. A more complete list of the post-9/11 security changes is presented in Table 3-7. The security changes are grouped into five categories, as follows:

- **Changes in Procedures**—These types of changes were most commonly implemented by trucking companies in the post-9/11 period. These changes included such specific measures as development of anti-terrorist policies, security coordination with vendors, re-evaluation

[12] The ATA HWP is funded by FMCSA as a national safety outreach initiative that trains drivers to report incidents (e.g., accidents, stranded motorists, poor signage, and/or suspicious activities at bridges, tunnels) to an operations center that forwards reports to the appropriate authorities. ATA has proposed that this program could function as the "Highway Information Sharing and Analysis Center" (H-ISAC) and could provide two-way communication with U.S. DOT's Transportation Information Operations Center (TIOC).

TABLE 3-7 Post-9/11 trucking industry security measures

Security Measures Implemented After 9/11	Number of Respondents	Percent of Total
Established terrorism policy; increased security awareness/training programs for employees.	10	53%
Issued employee ID/photo ID badges.	10	53%
Employee awareness and training bulletins/communications.	7	37%
Re-evaluated current systems.	6	32%
Greater scrutiny of potential and current employees (e.g, non-U.S. citizens were submitted to FBI for review).	5	26%
Increased internal physical security measures.	5	26%
Additional use of padlocks and cable seals.	4	21%
Worked with vendors/customers regarding different criteria relating to security.	4	21%
Cargo security policies for vendors/customers.	3	16%
Improved hazardous materials preparedness.	3	16%
Stricter routing of hazardous materials.	3	16%
Added security department—have policies and procedures.	2	11%
Hazardous materials customer and operator review.	2	11%
Implemented food chain security.	2	11%
Increased cargo inspections and response to suspicious packaging.	2	11%
Security load code; trailer hook-up for roadmen.	2	11%
Work with FBI, state, local authorities with policies and procedures in place.	2	11%
Added discharge clause for non-compliant drivers.	1	5%
Additional identification required at our terminals.	1	5%
Customs-Trade Partnership Against Terrorism (C-TPAT)	1	5%
Delays to be reported to and by customers.	1	5%
Deliveries in well-lit areas only.	1	5%
Driver authority to refuse questionable shipments.	1	5%
Increased use of guards.	1	5%
Installed GPS locators in all new trucks to track in case of theft.	1	5%
None.	1	5%
Review by U.S. DOT inspectors.	1	5%
Security cameras used for trailer compounds 24/7.	1	5%
Significantly cut back on loaded trailers left at facilities.	1	5%
Some customers requested that drivers wear ID badges.	1	5%
With HAZMAT loads, drivers not to stop—timed deliveries.	1	5%
Worked with American Chemical Council to find ways to reduce risk.	1	5%

TABLE 3-8 Post 9/11 security measures instituted by shippers and consignees

Security Measures Instituted by Shippers/Consignees After 9/11	Number of Respondents	Percent of Total
Chemical industry requirement for "responsible care" to protect product, employees, and public through proper handling/transportation of goods.	3	16%
Tighter seal controls on trailers transporting food and other products.	2	11%
Clients ask for certification and proof/criminal investigations for drivers and other employees before hiring firm for some assignments.	1	5%
C-TPAT is the main focus of many shippers; access and freight accountability is enhanced.	1	5%
Done very little; received copy of their security procedures.	1	5%
Enhances our operations as our employees follow the same procedure with each customer.	1	5%
Positive ID of drivers.	1	5%
Specific sealing observations.	1	5%
Tighter qualifications for drivers transporting HAZMAT.	1	5%

of cargo-related security, improved preparedness, and so forth. In addition to the survey responses, ATA has stated that some carriers are evaluating specific routes to be used and advising drivers transporting certain hazardous materials to avoid highly populated areas. Other procedural changes include driver verification of seal integrity at each stop, immediate notification of central dispatch if seal integrity is compromised, and reconciling the serial number on loaded trailers with the number on the shipper's documents prior to departure.

- **Employment-Related Practices**—These include greater scrutiny/background checks of existing and new employees, issuance of ID badges, and stricter discharge clauses. In addition to the survey responses, ATA has stated that some carriers now designate specific drivers for specific types of loads (e.g., hazardous materials).
- **Employee Training**—Some respondents have provided new training to improve security awareness and preparedness. This may include instructing drivers not to stop or render assistance except in the case of clear emergencies; alerting drivers to possible ploys used in vehicle hijackings; and advising drivers to notify their supervisors of suspicious shipments, or if necessary, to contact law enforcement to request inspection of shipments.
- **Physical Security**—Measures were implemented to improve facility security (e.g., cameras and guards), and vehicle and cargo security (e.g., locks and seals).
- **Addition of Technology**—Only three survey respondents specified the addition of technology-based measures in response to 9/11. These measures were cameras, locks and seals, and global positioning satellite (GPS) locators. However, the addition of new technology is a commonly mentioned planned measure, as discussed later.

As listed by both ATA and FBI sources, procedural security improvements may include actions such as not listing products

TABLE 3-9 Summary of what other trucking industry members are doing

What Other Trucking Industry Members Are Doing	Number of Respondents	Percent of Total
Presumably the same—proactive approach.	7	37%
They shouldn't tell us what they do so it isn't compromised.	3	16%
Each group wants its own ID source; recommend biometrical card for portion of the commercial driver's license (CDL).	2	11%
Secure trailer facilities—fences, gates, and 24/7 security guards.	2	11%
Securing trailer compounds with 24/7 cameras.	2	11%
Trucking companies willing to provide more security/technology—are customers willing to pay?	2	11%
U.S. DOT also provides alerts to us for security issues/warnings.	1	5%
Retraining staff and drivers on cargo/terminal security.	1	5%
GPS tracking of equipment.	1	5%
National Tank Truck Carriers (NTTC) gives us notices re: security issues/warnings.	1	5%
Others use ID badges because customers want it; cards not fail-safe.	1	5%
Communication with over-the-road (OTR) drivers.	1	5%
Waiting for federal regulations.	1	5%

TABLE 3-10 Planned trucking security measures

Additional Security Measures Planned	Number of Respondents	Percent of Total
Evaluate facility to add fences, gates, and security systems.	7	37%
Closed circuit TV with remote view-in capability and digital recording/storage.	6	32%
Considering controlled access, electric/electronic gates, key code, cameras, etc.	6	32%
Additional in-house driver training.	4	21%
All trailers to have operator ID system locks and seals.	2	11%
Hiring additional contracted security.	2	11%
Improved driver communication.	2	11%
Increased awareness through meetings.	2	11%
None.	2	11%
Regular driver call in.	2	11%
Still under review.	2	11%
Adding second trailer door-locking system.	1	5%
Employee ID.	1	5%
GPS equipment tracking.	1	5%
Improve tank-opening security—electronic alarms and locks.	1	5%
Need to evaluate since new measures also include cost factor.	1	5%
Testing devices to secure vehicle in event of terrorist attack.	1	5%
We are awaiting Homeland Security office guidance.	1	5%
If None, Why?		
Waiting on standardization from customers and government.	1	5%

TABLE 3-11 Trucking industry security technologies

Technologies Employed to Address Security Issues	Number of Respondents	Percent of Total
Information Technology (IT) systems.	5	26%
Closed circuit TV with digital recording/storage and remote view-in for selected locations.	4	21%
Currently have locks and padlocks at terminals when not in use.	3	16%
Electronic ID card.	3	16%
Electronic/electric access gates/perimeter security fences.	3	16%
Increased awareness, personnel training.	3	16%
Considering GPS, code entry requirement.	2	11%
Electric fences with guard dogs.	2	11%
Guard services and alarm systems.	2	11%
Investigating needs at terminals re: security issues.	2	11%
Liquid fleet use wireless communication and tracking products for communications with drivers.	2	11%
Locks and seals; need to upgrade quality of tamper-evident seals.	2	11%
Wireless communications and alarm systems.	2	11%
Cell phone/3-way radio.	1	5%
Concerned overall with the ways technologies are being employed.	1	5%
Covert CCTV and detection devices; burglar/fire alarms.	1	5%
Due diligence on prospective customers.	1	5%
Enhanced lighting.	1	5%
Newsletters.	1	5%
Trailer security protocol.	1	5%
Using GPS; enhanced physical security.	1	5%
Vehicle/cargo tracking devices.	1	5%
We pick up from the piers; use x-ray technology.	1	5%

by name on bills of lading or invoices given to the driver. Drivers often do not need to know what is being hauled and do not need access to loading areas where they can see the product. Shipping personnel can be instructed to not discuss products or operations with drivers, and trucking companies can be required to provide a driver's name and other identifying information prior to his or her arrival. Before release of pick-ups, tractor and trailer licenses should be recorded and checked against the company that is supposed to pick up the load, and a record of the driver should include both text (e.g., date of birth and other driver's license information) and nontext identifying information (such as photo or thumbprint of the driver).

As discussed in Section 3.2.2, there are U.S. DOT, U.S. EPA, and DoD regulations and industry recommendations that address trucking industry security measures. These are often based on safety concerns, but they can also mitigate terrorist threats. As a result of 9/11, DoD has released new regulations,[13] and U.S. DOT has published a proposal for new regulations.[14] The former represents post-9/11 changes that companies transporting military cargo have had to make. The proposed new U.S. DOT regulations suggest changes that trucking companies may need to make in the near future.

None of the respondents mentioned being part of the HWP, which is one of the foundations of the ATA's ATAP.[15] In the spring of 2002, this program was operating in only 6 states, but by the spring of 2003, the program had expanded to a total

[13] *Defense Transportation Regulation (DTR) DoD Regulation 4500.9-R-Part II Cargo Movement*, Ch. 205; updated April 2002; www.transcom.mil/J4/j4lt/dtr.html.

[14] *Federal Register*, July 16, 2002, Vol. 67, No. 136, pp. 46622–46624.

[15] "The American Trucking Industry's Anti-terrorism Action Plan," American Trucking Associations, Alexandria, VA, May 2002.

of 15 states, with more states expected in the near future. The ATAP was designed to coordinate industry and government efforts, and it includes specific steps that are to be taken under each of DHS's color-coded terrorist threat conditions.

With regard to the security requirements placed on truck operators by their clients as a result of 9/11, respondents report additional requirements placed on them by the chemical industry in the form of "responsible care" and tighter seal controls on food and other product shipments (Table 3-8). The chemical industry "responsible care" guidance was developed by the American Chemistry Council in conjunction with the Chlorine Institute and the National Association of Chemical Distributors.[16] These guidelines provide few specific recommendations but state that member companies must identify and assess security risks, implement additional security measures (e.g., the installation of physical barriers and additional screening of transportation providers), improve cyber as well as physical security, document security procedures, provide awareness training, and so forth. Other requirements placed by clients include the pre-approval of drivers, tighter qualification of drivers transporting HAZMAT, and presentation of a valid driver's license or identification card.

Most of the respondents assume that other companies are generally taking the same measures as they are and, therefore, provide little added insight into security-related activities of other industry members. The specific measures listed are generally the same as those listed under pre- and post-9/11 security measures (Tables 3-5 and 3-6), including the addition of GPS, communications systems, physical security measures, and training. An additional post-9/11 security measure reported to be implemented by other trucking companies was the use of biometric cards. Two respondents noted that there are many security measures available and that the trucking industry is willing to implement them if the customers are willing to pay for them.

Future plans for additional security measures reflect the industry's general belief that more needs to be done to ensure trucking safety. Unlike measures taken to date, planned security measures take greater advantage of available technology solutions. The planned changes presented in Table 3-10 are grouped into the following three categories:

- **Technology-based Measures**—These plans dominate the responses and, as such, differ from measures already implemented. The specific technology-based measures listed include closed-circuit/remote monitoring, electric and electronic gates, GPS and other tracking systems, added communications, alarms, and so forth.
- **Physical Security**—These plans include measures to improve facility security, vehicle and cargo security (locks and seals), the addition of guards, and so forth.
- **Communication**—Better communication is planned through the addition of meetings to improve awareness and more frequent on-road communications.

Some trucking companies have no plans for new security measures, whereas others are still evaluating their future needs or are awaiting standardization of requirements or specific guidance from relevant governmental agencies. Petroleum companies, for example, are evaluating national electronic access cards for entry to loading facilities.[17]

A broad range of security-related technology options is available to the trucking industry. Essentially, technology options and availability do not appear to limit trucking security. Technology options include the ability to track vehicle location and performance (e.g., speed and fuel use), monitor vehicle and trailer access, and maintain communication with drivers. These technologies are often based on satellites or computers and can be used openly or covertly. They can be used to monitor operations in real time or to record operations to be monitored at another time. These technologies can also be continuously used, scheduled for use, or used on an as-needed basis. There are technology options to implement virtually any form of monitoring, communication, tracking, and recording, in any combination and format needed. Many of these technologies are noted in either the survey responses on currently employed security technology (Table 3-11) or the responses on planned security measures (Table 3-10). A list of trucking industry technologies follows in order of reported frequency of use (most frequent to least frequent) by survey respondents:

- **Monitoring Technologies**—Closed circuit television (CCTV), digital recording, remote viewing, covert CCTV, and detection devices (e.g., motion, fire, and burglar sensors).
- **Access Control**—electronic access, gates, electric fences, ID cards, coded lock/entry, truck and trailer locks, seals and tamper sensors, remote engine shut-off, and identification or password for engine start-up. Some of these function independently, in redundant modes, or in tandem with other manual or technology-based options (e.g., electronic fence with Cable TV [CATV] and with guard dogs).
- **Tracking Systems**—Systems based on information technology (IT), satellites, or wireless GPS.
- **Communication**—Two-way radios, panic buttons, and cell phones.

[16] "Responsible Care Security Code of Management Practices," American Chemistry Council in conjunction with the Chlorine Institute and National Association of Chemical Distributors. www.americanchemistry.com.

[17] "Statement of Joseph M. Clapp, Administrator, Federal Motor Carrier Safety Administration, Before the House Committee on Appropriations Subcommittee on Transportation," February 13, 2002 (testimony). www.fmcsa.dot.gov/Aboutus/testimonies/2_13_02Clapp_Testimony.htm.

All trucking survey respondents listed some form of current access control, ranging from padlocks and guard dogs to electronic access gates and alarms. Roughly a third of the respondents currently employ some form of tracking technology, and nearly a quarter listed monitoring technologies. The surveyed companies are generally larger in size than the average trucking company; therefore, the more sophisticated and costly technologies, such as tracking and monitoring, may be less common in the industry as a whole than indicated by this survey.

Trailer seals are one of the few common technologies listed above for which there are some specific recommendations. The primary purpose of seals is to ensure the integrity of the load and prove that it was not tampered with once the seal was placed. Thicker bolt seals are more difficult to cut and thus provide greater security; however, all seals may be circumvented by actions such as removing doors or breaking the hasp and slipping the seal out. Indeed, there is virtually no security technology that cannot be circumvented. An example of this was seen when the 9/11 terrorists rapidly disabled the aircraft transponders that provide location and altitude, leaving radar as the only means for tracking aircraft location and no means for discerning aircraft altitude. It would not be possible to track a truck or trailer location after disabling a GPS or transponder-type system (radar cannot be used). Thus, trucking industry organizations, such as the ATA, maintain that performance standards can provide more important antiterrorism measures than specific technologies.[18]

However, there is acceptance of a role for security technology. The ATA ATAP includes evaluations of technologies that could possibly assist the trucking industry to effectively improve the security of trucks, terminals, and other operations. Given the wide variety of technologies available and multiple vendors for similar technology, evaluations of technological options are important for trucking companies to confidently invest in security technology. However, the lack of the survey responses mentioning relevant ATA programs and suggestions for security improvements (e.g., periodic security briefings on ATA websites such as www. truckline.com) suggests that widely conveying the findings of such evaluations may be the more difficult task.

FMCSA, in cooperation with FHWA and the U.S. DOT Joint Program Office for Intelligent Transportation Systems, has begun to examine the potential effectiveness of several technologies as part of an Intelligent Transportation System (ITS). The tests involve 100 HAZMAT trucks over a 2-year period. The purpose is to assess the effectiveness of different technologies and procedures and determine costs and benefits with respect to the safety and security of hazardous materials. Tested technologies include biometric driver verification to allow law enforcement, shippers, and consignees to make positive identifications of truck drivers; prevention of unauthorized drivers from operating a vehicle; off-route vehicle alerts; stolen vehicle alerts; cargo tampering alerts; and remote engine shut-off.[19]

Although security technologies listed in this report are associated with terrorist-related threats, few, if any, of these technologies were implemented solely to mitigate terrorism. All of the technologies mentioned are dual-use technologies and were adopted either for their cargo theft deterrence value or in response to a specific client request. Available technologies that may identify national security threats such as radiation detection devices, explosion detection devices, nonintrusive X-ray and gamma ray inspection systems, and other cargo-recording devices were not listed by the respondents.

3.2.6 Identification of Issues or Problems Associated with the Implementation and/or Use of Specific Security Measures

Industry problems or issues associated with implementation of security measures were assessed based on responses to the question: *What problems or issues did you experience with the implementation and/or use of specific national security measures or technologies?* Responses to this question are presented in Table 3-12.

The most common comment relates to the overall cost of adding, maintaining, and using new technologies. Purchase costs or leasing fees, service, training, facility, and other incidental items are some of the key cost components noted. A large number of respondents report no critical problems or issues or list access and infrastructure issues (e.g., cannot fuel or have no access to facilities). Employee concerns of privacy invasion are also noted. Other difficulties in technology implementation include the constant need to evaluate the large number and changing nature of technology options, the lack of standardization, and a lack of consistency in customer needs.

3.2.7 A Summary of Security Research and Development Related to the Commercial Trucking Industry and What Other Research Would Be Beneficial

Three survey questions addressed the industry perception of what research is being done that may be relevant to the commercial trucking and bus industries. These questions were: *(1) What research is being done that would assist you in meeting your national security needs? (2) What assistance, research, development, training, technology, and other activities or services would help you in achieving the desired and*

[18] "The American Trucking Industry's Anti-terrorism Action Plan," American Trucking Associations, Alexandria, VA, May 2002.

[19] "The American Trucking Industry's Anti-terrorism Action Plan," American Trucking Associations, Alexandria, VA, May 2002.

TABLE 3-12 Trucking industry problems with implementing technologies

Problems/Issues with Implementing Technologies	Number of Respondents	Percent of Total
Overall cost.	13	69%
None.	7	37%
Constantly evaluating technologies (e.g., remote engine shut down).	2	11%
Employee mistrust.	4	22%
Varying requirements by the customer base.	2	11%
Human element—people forgetting to do tasks (swapping out videotapes from VCRs).	1	5%
Lack of consistency in the chemical shipping industry.	1	5%
With military shipments cannot fuel up at terminals, must use truck stops.	1	5%
Military holding facilities lack adequate facilities for drivers, who must use truck stops.	1	5%
Mostly technological glitches with new systems.	1	5%
Need to standardize cargo seals to meet customer requirements.	1	5%

necessary level of security? Who should provide these needs? (3) What organizations do you and your industry rely on for the development of national (anti-terrorism) security measures (procedures, technology, training, etc.)? Tables 3-13, 3-14, and 3-15 present responses to these questions.

The information provided by the survey respondents suggests that trucking companies are not well versed in ongoing research efforts. The responses provided in Table 3-13 do not identify specific "research in progress" that would assist the industry in meeting its security needs. The items listed (e.g., GPS-tracking equipment, biometric cards, and communications) are currently available as commercial products. Survey respondents did not provide specific areas for improvement of these products. Recommendations for efforts to reduce the costs of technological options were not voiced; however, as seen in Table 3-12, cost is identified as a problem for implementation of technology options.

TABLE 3-13 Trucking industry security research

Research in Progress to Assist in Meeting Security Needs	Number of Respondents	Percent of Total
GPS tracking of equipment.	3	16%
They shouldn't tell to avoid compromising security.	3	16%
Each group wants its own ID source; recommend biometrical card for portion of the commercial driver's license (CDL).	2	11%
National Tank Truck Carriers (NTTC) gives us notices re: security issues/warnings.	2	11%
Others use ID badges because customers want it; cards not failsafe.	2	11%
Presumably the same—proactive approach.	2	11%
Secure trailer facilities, fences, gates, 24-7 security guards.	2	11%
Trucking companies willing to provide more security/technology—are customers willing to pay?	2	11%
U.S. DOT provides alerts to us for security issues/warnings.	1	5%
Communication with over-the-road (OTR) drivers.	1	5%
Retraining staff and drivers on cargo/terminal security.	1	5%
Securing trailer compounds with 24/7 cameras.	1	5%
Waiting for federal regulations.	1	5%

TABLE 3-14 Desired trucking industry security research

Research Desired to Enhance Security Measures	Number of Respondents	Percent of Total
Need a federal operator ID program so employers can exchange information without fear of litigation.	5	26%
More technology for product security—alarms, self-locking cargo compartments; believe the private sector will lead the way.	2	11%
Need uniform instructions and have everyone "on the same page."	2	11%
"Wait and see" new government regulations; future terrorist actions may dictate.	1	5%
Better engineering of trailers with less susceptibility to contamination.	1	5%
Learn from ATA.	1	5%
Need awareness training; teach trucking companies/ drivers to be observant.	2	11%
Need standardization of sealing practices.	1	5%
Need to be aware of economic terrorism.	1	5%
Secure "loose borders."	1	5%

The trucking industry survey respondents' desires for research, development, training, technology, and other activities or services to help achieve the desired level of security are listed below, along with a brief description of programs currently underway to address these issues (Table 3-14):

- Development of a uniform federal operator (driver) identification system to enable national-level tracking of

TABLE 3-15 Organizations used for developing trucking industry security measures

Organizations Relied Upon for Developing National Security Measures	Number of Respondents	Percent of Total
American Trucking Associations.	10	53%
National Tank Truck Carriers Association (NTTC).	5	27%
American Chemistry Council.	4	21%
National Cargo Security Council.	3	16%
State trucking associations.	3	16%
Work with federal, state, and province enforcement agencies.	3	16%
Chambers of Commerce.	2	11%
FMCSA.	2	11%
Transportation Research Board (TRB).	2	11%
American Society for Industrial Security.	1	5%
Business Roundtable.	1	5%
Cargo Criminal Apprehension Team (CATS).	1	5%
Commercial Vehicle Safety Alliance.	1	5%
CTAP.	1	5%
ENO Foundation.	1	5%
FAST.	1	5%
Federal Bureau of Investigation.	1	5%
Intermodal Association of North America (IANA).	1	5%
Internal experienced security personnel.	1	5%
Security companies	1	5%
Manufacturers.	1	5%
Midwest Cargo Security Council.	1	5%
Own—large law-enforcement, legal & safety departments.	1	5%
Transportation groups.	1	5%
Transportation Loss Prevention and Security Association.	1	5%
U.S. Customs.	1	5%
Web-based equipment tracking companies.	1	5%

drivers. The U.S. DOT/TSA TWIC program, described in Section 3.2.3, is a federal transportation worker identification system. The details of TWIC are currently under development, but the goal of this program is to provide a uniform driver ID system.

- Development/improvement of specific access control technologies, including alarms, self-locking cargo compartments, improved trailers, and standard sealing practices. As listed in Section 3.2.5, control technologies including alarms, self-locking cargo compartments, and seals are commercially available; however, these technologies can be circumvented. The competitive nature of the security products industry encourages continued product improvements.
- Awareness training. Awareness training is provided as part of the ATA HWP, and the availability of this training is likely to increase as the HWP expands.
- Improved border security. As discussed in Section 3.2.8, efforts currently are underway to improve border security and efficiency.

Table 3-15 contains the responses identifying the organizations that trucking companies rely on for information on anti-terrorist measures. Industry associations are frequently listed (e.g., ATA, NTTC, American Chemistry Council, National Cargo Security Council, and individual state trucking associations). The listed federal agencies include FMCSA, the FBI, and the U.S. Customs Service. None of the survey respondents listed for-profit companies that offer security and anti-terrorism manuals, seminars, videos, and so forth.

3.2.8 Information on What Has Been Done in Other Countries to Enhance the Security of Commercial Truck Safety, Particularly in Countries That Have Had to Deal with Significant Terrorist Activity

Industry knowledge of security procedures in other countries was assessed from survey responses to the question: *Can you comment on what has been done in other countries to enhance the security of commercial truck safety?* Responses to this question are presented in Table 3-16.

The responses in Table 3-16 do not include specific anti-terrorist security measures practiced in other countries. They do report some awareness of general security shifts in Canada and some technical developments in Europe and elsewhere. These technical developments include making containers more secure, off-route GPS, accident warning devices, bumper/brake, and remote vehicle shut-off systems.

Additional information on trucking security measures employed in other countries was obtained from interviews with selected embassy personnel. Israel, India, and Russia were of particular interest because of the relatively high incident rate of terrorist acts in these countries. Mexico and Canada were of interest because of their shared borders with the United States. The Israeli and Russian embassies would not comment on their truck-related terrorism concerns or their anti-terrorism measures.

TABLE 3-16 Trucking industry security measures used in other countries

Awareness of Other Countries' Enhanced Security Measures	Number of Respondents	Percent of Total
Unknown.	9	47%
We transport into Canada regularly; we're aware of changes at the border crossings; tightened down security.	3	16%
Aware of European high-tech initiatives on securing containers; Europe is advanced, and we need to catch up.	2	11%
Aware of Israel's lack of success with trucks, buses, ambulances—any mode that carries people into areas of interest or population.	1	5%
Aware of other countries not nailing down physical assets and not being able to make sure that the wrong people don't get a hold of it.	1	5%
Emphasis is being placed on safe transportation and security of overseas containers.	1	5%
Have very limited knowledge exposure to Mexican border crossings.	1	5%
Off-route GPS, satellite/cellular notifications.	1	5%
Radar, sonar, infrared warning devices for accident prevention (fog).	1	5%
Rear bumper brake activation for law enforcement.	1	5%
Remote vehicle shut-off systems.	1	5%
Some state the criterion is "overkill" in the industry, especially when forced on the industry by insurance carriers.	1	5%
These issues are just now being addressed 1 year after 9/11.	1	5%
Tracking/securing devices through remote operations.	1	5%

The Indian embassy provided some comments on how the Indian government addresses terrorist use of trucks.[20] Recent terrorist acts using trucks in India have included the detonation of explosive devices planted on trucks and setting coal trucks ablaze. Terrorist threats using trucks are often directed at passengers as terror tactics. The use of trucks to transport terrorist weapons and personnel is also an issue. In addition, so-called "taxes" are levied on trucks using routes in terrorist-dominated areas. Federal legislation and security resources are implemented and used by local and state governments, who provide the front-line address of terrorist risks. Cost-benefit analyses determine the technology and security measures along different routes. The events of 9/11 had little effect on anti-terrorism strategies in India, largely because they have been dealing with repeated terrorist attacks throughout the last decade.

With respect to countries bordering the United States, alerts from U.S. Customs issued immediately after 9/11 resulted in

[20] Mr. Jayanto Choudhury, Counsellor, Embassy of India, Washington, D.C.

extreme delays in border crossings. On the Canadian border, U.S. Customs has minimized these delays by implementation of technological solutions such as the International Trade Data System (ITDS) and the Automated Commercial Environment (ACE). These systems allow carriers to pre-file cargo, conveyance, and crew data for risk assessment by federal agencies prior to arrival at border crossings. Additionally, the U.S. and Canadian governments signed a 30-point Smart Border Declaration in December 2001 that lists key areas for cooperation in border policy. Harmonization of customs procedures and more secure and efficient border crossings are the subject of ongoing discussions.

Customs administration between Mexico and the United States has been fully automated since 1991. After 9/11, the United States and Mexico signed the U.S.–Mexico Border Partnership Action Plan to promote cooperation and the use of technology to provide secure and efficient border crossings. This includes the continued development of a joint intra-transit shipment tracking system and implementation of the Container Security Initiative.