UN/SCETDG/21/INF.19

COMMITTEE OF EXPERTS ON THE TRANSPORT OF DANGEROUS GOODS AND ON THE GLOBALLY HARMONIZED SYSTEM OF CLASSIFICATION AND LABELLING OF CHEMICALS
Sub-Committee of Experts on the Transport of Dangerous Goods
(Twenty-first session, 1-10 July 2002,
agenda item 12)

OTHER BUSINESS

Transport Security

Transmitted by the expert from the United States of America

1. The expert from the United States of America provides this paper in relation to ST/SG/AC.10/C.3/2002/56 by the Secretariat for the information of the Sub-Committee. ST/SG/AC.10/C.3/2002/56 reproduces statements by the Secretariat on transport and security that were submitted to the United Nations Economic Commission for Europe Inland Transport Committee. The paper indicates that both the United Nations General Assembly and the United Nations Security Council have called for intensified international cooperation and action to prevent and suppress terrorist acts. The paper identifies issues that might benefit from additional security considerations. The welcomes the efforts by the Secretariat to highlight the importance and seriousness of this matter. In the area of dangerous goods transport, the paper identifies security measures that can be taken with respect to the transport of dangerous goods. These are measures that are being considered in the United States of America to integrate security into safety regulations. We agree that States should provide the secretariat with information on steps being taken to enhance security.

2. As a result of the terrorist attacks on the World Trade Center and the Pentagon on September 11, 2001, and subsequent terrorist threats, the United States of America has undertaken a broad review of government and industry dangerous goods transport safety and security programs. In the wrong hands, dangerous goods pose a significant security threat. While current dangerous goods regulations generally provide for a high degree of safety with respect to avoiding and mitigating unintentional releases of dangerous goods in transport they do not specifically address security threats. Dangerous goods shippers and carriers must take action to enhance dangerous goods transportation security. Persons who offer, transport, or store dangerous goods should develop and review their current security measures. The expert from the United States of America is interested in sharing information on actions that are being considered and taken to enhance security relevant to the transport of dangerous goods and is providing information relevant to steps being taken in the United States. We have identified a number of actions that persons involved in the transport of dangerous goods can implement to enhance security. These actions are not government regulations or mandates and are not intended to be inclusive but have been recommended to enhance the safe and secure transport of dangerous goods. These are included in Annex 1 to this paper.

3. The United States of America is taking steps to integrate security requirements into its dangerous goods safety regulations. We recently published proposed regulatory amendments to the United States of America national regulations to enhance the security of dangerous goods shipments. The proposed requirements include the development of security plans by shippers and carriers and security training for employees engaged in dangerous goods transport. The proposed amendments can be accessed via the Internet at http://hazmat.dot.gov/rules/67fr-36168.htm.

Annex 1 - Security Enhancement Recommendations for Shippers and Carriers

I. Security Plans

The most important action a shipper or carrier should consider is the development and implementation of a security plan. Shippers and carriers should use a risk management model to assess security risks and develop appropriate measures to reduce or eliminate risk. Most risk management models utilize the following steps:

- Identify areas of concern and partners that may be affected or with whom coordination may be appropriate;
- Assemble detailed information on system operations;
- Identify control points where interventions can reduce or eliminate risk;
- Select and prioritize options to meet identified security goals;
- Take action to implement the strategy;
- Verify implementation of the strategy; and
- Evaluate the effectiveness of the strategy to determine whether additional actions are necessary.

The first step in developing a security plan should be to develop a list of the dangerous goods that are transported and identify those dangerous goods with the potential to be used as weapons of mass destruction or targets of opportunity. Then, consider a review of current activities and operations from a transportation security perspective. Shippers and carriers need to undertake a self-assessment of: ``What they are doing now? What could go wrong? What are the vulnerabilities? What can they do differently to prevent terrorist actions?" The next step is to consider how to reduce the identified risks. For dangerous goods transport, a security plan likely will focus on personnel, facilities and en route security issues. To assist shippers and carriers in developing effective risk assessments, the United States of Americahas posted a Risk Management Self-Evaluation Framework on its hazardous materials safety website (see http://hazmat.dot.gov/risk.htm or http://hazmat.dot.gov/rmsef.htm).

II. Personnel Security

Realizing that transport workers can serve as a critical element of any security program, the United States of Americais recommending that shippers and carriers take one or more of the following actions:

- Assure employees are familiar with the security plan and are properly trained in its implementation. Training should include company security objectives, specific security procedures, employee responsibilities, and organizational security structure;
- Employees should be encouraged to report suspicious incidents or events to management. Routine security inspections should be implemented. Regular employee/management meetings on security measures and awareness should be convened;
- An internal communication system to inform employees of events, facts, trends, updates, and the like should be implemented and because Internet communications may be accessed by others, alternative methods for communicating sensitive information should be used; and
- Since employees may pose a potential security risk, employers should consider establishing a process to verify the information provided by job applicants on application forms or resumes, including checking with former and current employers and personal references provided by job applicants.

III. Facility Security

Shippers and carriers should consider taking one or more of the following steps to prevent unauthorized access to their facilities:

- Establish partnerships with local law enforcement officials, emergency responders and other public safety agencies. Through such relationships, you can learn about threats, trends, and successful and unsuccessful security programs;
- Request a review of their facility and security program by local law enforcement officials;
- Restrict the availability of information related to the facility and the dangerous goods that are stored, processed and transported. Encourage authorities in possession of information about the facility to limit disclosure of that information on a need-to-know basis;
- Add security guards and increase off-hours patrols by security or law enforcement personnel;
- Improve fencing around the facility. Check the adequacy of locks and other protective equipment. Consider equipping access gates with timed closure devices. Conduct frequent inspections. Install additional lights, alarm systems, or surveillance cameras;
- Restrict access to a single entry or gate;
- Place limits on visitor access; require visitors to register and show photo identification and have someone accompany visitors at all times;
- Require employees to display identification cards or badges;
- Conduct security spot checks of personnel and vehicles;
- Upgrade security procedures for handling pick-ups and deliveries at facilities. Verify all paperwork and require pick-ups and deliveries to be handled only by appointment with known vendors. Require vendors to call before a delivery and to provide the driver's name and vehicle number. Accept packages and deliveries only at the facility front gate;
- Secure hazardous materials in locked buildings or fenced areas. Have a sign-out system for keys. Secure valves, manways, and other fixtures on transport equipment when not in use. Lock all vehicle and delivery trailer doors when not in use. Secure all rail, truck, and barge containers when not in use. Use tamper-resistant or tamper-evident seals and locks on cargo compartment openings;
- Periodically inventory the quantity of dangerous goods on site in order to recognize if a theft has occurred;
- Keep records of security incidents. Review records to identify trends and potential vulnerabilities; and
- Report any suspicious incidents or individuals to local law enforcement officials.

IV. En Route Security

Shippers and carriers should work together to assure the security of dangerous goods shipments while in transport from origin to destination. Shippers should assess the transportation modes or combinations of modes available for transporting specific materials and select the most appropriate method of transport to assure efficient and secure movement of dangerous goods from origin to destination. Shippers should know their carriers and develop carrier profiles that include a system for qualifying the carriers used to transport dangerous goods. Use of carrier safety ratings, assessments, safety surveys, or audits and questionaires that require the carrier to provide information on security measures it has implemented is recommended. Shippers should verify that the carrier has an appropriate employee hiring and review process, including background checks, and an on-going security training program. They should verify the identity of each carrier and/or driver prior to loading dangerous goods onto a vehicle or offering them to the carrier. This should include asking the driver for photo identification and commercial drivers license and compare with information provided by the carrier. Shippers should ask the driver to provide the name of the consignee and the destination for the dangerous goods and confirm the carrier information with their records before releasing shipments.

Carriers should:

- Identify preferred and alternative routing, including acceptable deviations and should strive to minimize exposure of dangerous goods to communities or populated areas, including downtown areas; avoid tunnels and bridges where possible; and expedite transportation of the shipment to its final destination;
- Minimize stops en route;
- Select locations with adequate lighting on well-travelled roads when stopping is unavoidable;
- Check vehicles after each stop to make sure that tampering has not occurred;
- Consider using two drivers or driver relays to minimize stops during the trip;
- Avoid layovers, particularly for high hazard dangerous goods such as explosives, toxic gases or infectious substance;
- Cooperate with shippers to assure the security of rail cars, vehicles, portable tanks, freight containers and other transport packagings are stored temporarily when necessary in secure locations preferably on private property inaccessible to the public;

- Train drivers in how to avoid highjacking or stolen cargo--keep vehicles locked when parked and avoid casual conversations with strangers about cargoes and routes;
- Consider if a guard or escort for a specific shipment or hazardous material is appropriate;
- Consider utilizing advanced technology to track or protect shipments en route to their destinations. For example, by installing tractor and trailer anti-theft devices or utilizing satellite tracking or surveillance systems. As an alternative, carriers should consider frequent checks with drivers by cell phone to ensure everything is in order;
- Install tamper-proof seals on all valves, vehicle or container openings;
- Establish a communication system with transport vehicles and operators, including a crisis communication system with primary and back-up means of communication among the shipper, carrier, and law enforcement and emergency response officials;
- Implement a system for a customer to alert the shipper if a dangerous goods shipment is not received when expected;
- Notify law enforcement personnel if they suspect that someone has shipped or delivered dangerous goods to someone who may intend to use it for a criminal purpose; and
- Report any suspicious incidents or individuals to law enforcement officials.

V. Additional Information

Up-to-date information is a key element of any security plan. Shippers and carriers should consider methods to:

(1) Gather as much data as possible about their operations and those of other businesses with similar product lines and transportation patterns;
(2) Develop a communications network to share best practices and lessons learned;
(3) Share information on security incidents to determine if there is a pattern of activities that, when considered in isolation are not significant, but when taken as a whole generate concern; and
(4) Revise security plans as necessary to take account of changed circumstances and new information.
