U.S. Department
of Transportation

**Research and
Special Programs
Administration**

Enhancing Security of Hazardous Materials Shipments

Against Acts of Terrorism or Sabotage

Using RSPA's

Risk Management Self-Evaluation Framework (RMSEF)

January 2002
Revision 1

This template or overlay for the Risk Management Self-Evaluation Framework applies the methodology to the issue of security. It is a tool and not a regulatory requirement. Its use, like that of the basic framework, is voluntary.

We would appreciate feedback on your experiences using this template and suggestions for improvement. Comments should be provided to the U.S. Department of Transportation's Research and Special Programs Administration, Office of Hazardous Materials Technology, DHM-20, 400 7th Street, S.W., Washington, DC 20590 or by accessing our website at http://hazmat.dot.gov/risk.htm.

RMSEF SECURITY TEMPLATE

Enhancing Security of Hazardous Materials Shipments Against Acts of Terrorism or Sabotage Using RSPA's Risk Management Self-Evaluation Framework (RMSEF)

I. RMSEF and Hazardous Materials Transportation Security

Given the heightened specter of terrorism, the security of hazardous materials (hazmat) shipments has become a priority for carriers, shippers, consignees, emergency responders, and government officials. The existing hazmat transportation process, including personnel, procedures, and facilities/equipment needs to be reexamined with a security focus. Addressing such security concerns should be part of an overall strategy to manage the risk of hazardous materials during transportation. Now an existing tool from the Research and Special Programs Administration's (RSPA) Office of Hazardous Materials Safety (OHMS) can be used by carriers, shippers, consignees, emergency responders, and government officials to enhance security and safeguard shipments of hazardous materials against terrorist attacks or sabotage. The Risk Management Self-Evaluation Framework (RMSEF) is a voluntary tool that helps evaluate and manage the risks associated with transporting hazardous materials in a proactive manner. A company or organization knows what works best for itself; RMSEF provides a structured way of assessing risk and helping hone practical, common-sense knowledge to reduce risks even further. RMSEF is applicable to all transportation modes and is flexible enough to provide the framework needed to evaluate and mitigate security risks.

II. RMSEF Principles Applied to Managing Security Risk

RMSEF outlines the following fundamental principles that are critical for successfully managing risk. As tailored to security, the principles include:

- Obtaining **commitment** to reducing security risks on the part of both managers and workers.
- Promoting a "risk reduction **culture** with a security focus" in day-to-day operations.
- **Partnering** with all parties involved in securing the hazardous materials transport chain.
- **Prioritizing** security risks so that resources can be allocated effectively.
- Taking **action** to reduce the security risks that have been identified.
- Striving for **continuous improvement**.

- **Communicating** with all parties to ensure each knows its role and is aware of relevant security risk information.

III. RMSEF's Stepwise Process Applied to Security Risk

Once the groundwork for risk management is laid by instilling the principles throughout a particular organization, RMSEF provides a systematic "stepwise process" to assess and reduce risks. The stepwise process is based on other risk management efforts and was developed through a collaborative effort between government, industry, and the public.

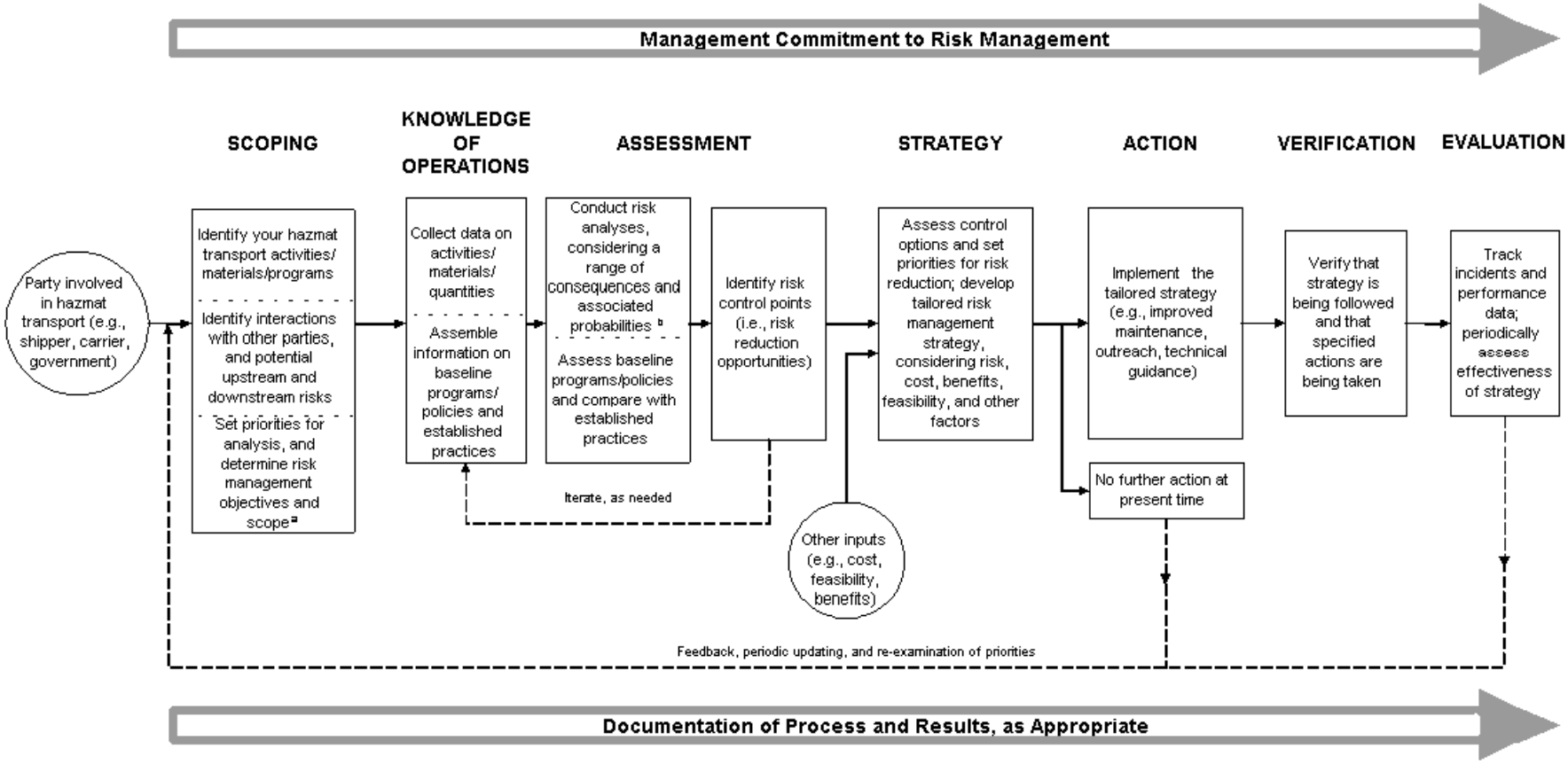
These steps of the RMSEF (see flowchart exhibit) are sufficiently general that the framework can be customized to address a variety of risk management issues and achieve measurable improvements. It is adaptable by shippers and carriers to systematically help in securing their hazardous materials shipments against acts of terrorism or sabotage.

Other methods for assessing and addressing security risk have been developed by government or private industry in specialized circumstances; however, none have a general focus on hazardous materials transportation. These methods differ in the source of their creation, the number of steps, and the scope of their activities. However, they share many steps common to the RMSEF (see Attachment 1). The following gives practical suggestions for ways in which each step of the RMSEF can be applied to protecting hazardous materials shipments from terrorist activity or sabotage. As shown in the exhibit below, management commitment and adequate documentation are essential to the risk management process.

Step 1: Scoping

Security considerations can cut across the entire hazmat transportation process. However, to effectively focus an effort on security risk, a company should generally characterize its hazmat transportation operations, and then make initial decisions as to which transportation activities should have more security scrutiny. The initial decisions could be made based on company perceptions regarding the greatest security risks or based on previous threats. For example, a shipper may decide that all of its hazardous materials shipments are vulnerable to terrorist attacks or sabotage, or perhaps it may narrow the focus to select chemicals with specific hazard potential (e.g., toxic gases). Similarly, a carrier may decide that its rail operations are more vulnerable to attack than its highway shipments. In light of concerns regarding the fraudulent use of Commercial Drivers' Licenses (CDLs) and hazardous materials endorsements, companies may wish to focus on their potential new employee screening process. Defining the scope of the activities to be considered in terms of security also includes identifying other partners (e.g., shipper, container manufacturer, local emergency response, law enforcement personnel, consignees) that are interested in the security of the company's hazardous materials transportation processes.

RISK MANAGEMENT SELF-EVALUATION FRAMEWORK



[a] Scope can vary from extremely broad, such as addressing an organization's entire hazardous materials operations, to very specific, such as targeted to a single material or transport route or to the type of risk (e.g., security).

[b] Analyses can be qualitative and quantitative, and are usually both.

Step 2: Knowledge of Operations

The next step of the RMSEF involves collecting detailed information about the hazmat transportation operations/decisions that will be examined for security risks. A company should describe the quantities of hazmat transported, who handles the materials, the routes used, and where and when they are handled. Additionally, a company should describe the existing security activities associated with these hazmat transportation operations. It is important to include security activities that were originally designed for security (e.g., fencing) as well as activities considered originally for safety or risk management (e.g., chlorine valve cap), but now have a security value. The inventory of information should cover security issues with personnel (e.g., background checks, licensing, training), security procedures and plans, and security of facilities and equipment. Current safety and risk regulations (e.g., parking restrictions) that have security impacts are also important to list. In determining the security activities to describe, a company may want to ask how are loads secured? Is there a forum for employees to constructively air grievances? Is there certainty that drivers actively follow the company's security guidelines? What are the chief causes of transportation-related accidents at the company? Have any threats previously been received by any company offices? Are there any trends that can be identified (e.g., regions or trailer types with a higher frequency of theft)? Having knowledge of existing security measures and transportation operations also enables a company to compare security measures with the industry and with recommendations by the government.

Step 3: Assessment

This assessment step involves analysis of a company's operations and characterization of the nature and magnitude of the security risks. The assessment does not have to be costly or complex, but can begin simply and progress in complexity as needed. It can simply involve reporting the impressions of experienced company staff, brainstorming, or conducting a survey by a diverse team composed of staff from various operations (e.g., risk managers, drivers, tank car vendors), or conducting more formal and rigorous hazard assessment techniques (e.g., use of risk matrices and scoring or ranking systems, fault tree analysis, or hazops). In any case, the goal is the same. A key element of this step is to identify points in the hazmat transportation chain where security risk exists, but where actions can be taken to reduce the security risk. These points are called risk control points. These risk control points can vary widely, including everything from changing driver training curricula, to increasing emphasis on load safety, to rethinking routing procedures or adding to existing emergency response protocols.

When selecting security risk control points, the following areas may require special attention:

- *Personnel backgrounds* (e.g., employment history and verification of citizenship or immigration status);

- *Hazardous materials and package control* (e.g., adequate lighting, locks, and security systems);

- *En route security* (e.g., avoidance of tunnels, high population centers);

- *Technical innovations* (e.g., appropriate access control systems, use of satellite tracking and surveillance systems);

- *Management prerogatives* (e.g., fingerprinting applicants during employment process);

- *Communications* (e.g., use of cell phones to reach all key personnel as well as risk communications for public and immediate reporting of suspicious activity or thefts to appropriate authorities);

- *Emergency Response* (e.g., adequacy of training and resources for response to terrorist type incidents); and

- *Readjustment based upon current conditions* (e.g., heightened security after initial terrorist attacks or in accordance with threat levels that may have been established by appropriate authorities).

Step 4: Strategy

The heart of a strategy to address security risks is to develop a security action plan. The plan prioritizes the security risk control points based on the degree of vulnerability and potential impact. The plan also outlines potential preventive and control actions based on the ability to reduce risk and the resources available. For example, if a company has a high turnover rate, it may decide to review employee rosters to ensure that comprehensive background checks have been performed on all individuals with particular scrutiny being applied to employees who have links to countries identified as supporting terrorist activities. Badges or personnel identification cards may be required for access to areas containing hazardous materials. Guard forces or fences at rail yards may be increased. Routing may be changed to avoid high population areas or to enable hazardous materials shipments to be delivered more rapidly. New locking mechanisms may be installed for fifth wheels so that trailers are less likely to be stolen, or electronic engine controls may be adjusted to require an entry code in addition to a key.

Additionally, the plan should have a schedule, assigned responsibilities and, most importantly, management commitment. The plan should be summarized in a written document.

Step 5: Action

This step involves implementation of the written plan developed in Step 4.

Step 6: Verification

After implementing the written plan, a monitoring protocol should be established to ensure that activities are proceeding according to plan. For example, third party inspectors (government or industry) can be requested to perform an independent evaluation of a company's vulnerability to terrorist attacks or sabotage. Any security breaches discovered during this evaluation would then need to be promptly addressed.

Step 7: Evaluation

This step determines if the goals established for reducing security risk for hazardous materials transportation are being met. To measure progress, a company needs to have relevant, cost-effective performance indicators. For example, logs tracking the incidence of theft or property damage can be monitored to determine whether significant improvements have resulted from implementation of the selected risk management strategies. Trade associations such as the National Tank Truck Carriers (NTTC) often assemble information on safety-related performance indicators that can be made available to their member companies. With set performance indicators, progress in meeting the goals and strategies can then be compared with performance indicators used by other companies in similar fields. Periodic reviews and assessment of existing plans should be scheduled.

IV. Specific Reference Information for Security of Hazardous Materials Transportation

Below is a list of reference materials that can be used to flesh out the RMSEF and tailor it more specifically to a company's needs. This is by no means an exhaustive list of the information available on this topic and interested individuals are encouraged to investigate additional resources. Suggested references are as follows:

- DOT's Hazardous Materials Safety Webpage: Provides the latest government alerts on terrorism. The website address is http://hazmat.dot.gov .

Information on the RMSEF's development, structure, and testing can be found at http://hazmat.dot.gov/rmsef.htm.

- Federal Motor Carrier Safety Administration Security Talking. Security talking points can be found at the DOT Federal Motor Carrier Safety Administration Website www.fmcsa.dot.gov/hazmatsecure.htm. The topics include general security information, personnel security, hazardous materials and package controls, en route security, technical innovations, management prerogatives, communications, and readjustment based upon current conditions.

- American Chemistry Council Webpage: Provides guidance on transportation security and guidelines on site security for chemical plants. The website address is http://www.americanchemistry.com .

- Transportation Research Board Security Webpage: Provides links to documents and other information on the following topics: general transportation security, aviation security, surface transportation security, seaport/maritime security, and general national security websites. The website address is http://www4.trb.org/trb/homepage.nsf/web/security.

- National Safety Council Webpage: Presents general safety information, including a document entitled "Effective Emergency Response Plans: Anticipate the worst, prepare for the best results." The website address is www.nsc.org/issues/emerg/99esc.htm .

- National Cargo Security Council Webpage: Provides theft prevention information, including a list of cargo security links and the document *Guidelines for Cargo Security & Loss Control: How to maximize cargo security on land, air & sea*, edited by Lou Tyska, CPP. The website address is www.cargosecurity.com .

- American Society for Industrial Security Webpage: Includes security information for industrial facilities, as well as a document entitled *Cargo Theft Prevention: A handbook for logistics security* by Louis A. Tyska, CPP, and Lawrence J. Fennelly. The website address is www.asisonline.org .

- American Trucking Associations (ATA) Webpage: Provides a host of information on government security warnings, security tips, and other guidance. Available documents include *Guidelines for Loss Prevention: Physical security in motor carrier freight terminals* and *Security and the Driver*, both authored by the Safety & Loss Prevention Management Council. The ATA website address is www.truckline.com. In addition, ATA hosts CargoTIPS, an interactive cargo theft information processing system available at www.cargotips.org.

- Agency for Toxic Substances and Disease Registry (ATSDR) Webpage: Provides information on general hazardous materials emergency response as well as strategies for mitigating and preventing terrorism involving industrial chemicals. The website address is http://cisat1.isciii.es/.

- U.S. Environmental Protection Agency (EPA)'s Counter-Terrorism Webpage: Provides publications, links, and alerts related to EPA's role in counter-terrorism. EPA's recommendations on chemical accident prevention and site security can be found at http://www.epa.gov/ceppo/pubs/secale.pdf . The website address is http://www.epa.gov/ceppo/cntr-ter.html .

- Department of Defense (DoD) Guidance on Security and Transportation. Although these DoD guidances are written specifically to ensure the security of nuclear, chemical, or conventional weapons during transportation, many of the practices are easily applicable to the transportation of other high-value loads, including hazardous materials loads. 1) Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (DoD 5100.76-M); 2) DoD Nuclear Weapons Transportation Manual (DoD 4540.5-M); and 3) Physical Security Program (DoD 5200.8-R). The website address is http://www.dtic.mil/whs/directives.

- National Institute of Justice and Sandia National Laboratories: Provides information on security, terrorism, and assessment methodologies. The website addresses are http://www.ojp.usdoj.gov/nij and http://www.sandia.gov, respectively.

Attachment 1

Other Security Methodologies

- **Chemical Facility Vulnerability Assessment Methodology**
  This methodology was developed by the National Institute of Justice in partnership with the U.S. Department of Energy's Sandia National Laboratories, with the cooperation and assistance of chemical industry representatives. It is a tool for assessing the potential security risks at chemical facilities, focusing on terrorist or criminal actions that could have significant national impact or could cause the airborne release of hazardous chemicals resulting in deaths and contamination. The assessment methodology contains twelve-steps that similar in many ways to those in RMSEF. A priority-ranking matrix helps determine risk levels and suggest adoption of features to address vulnerabilities when these levels are too high.

- **Assessment of Vulnerability to Attacks on the Physical Surface Transportation Infrastructure or on the Surface Transportation Information Systems and Network**

  The National Research Council was directed by Congress to establish research and development priorities for "defending against, mitigating the consequences of, or assisting in the investigation of attacks on the physical surface transportation infrastructure or on the surface transportation information systems and network." The methodology used to assess the vulnerability of these transportation assets consists of nine steps, which are primarily focused around the scoping, knowledge of operations, strategy, and assessment steps of the RMSEF.

- **ATSDR 10-Step Procedure for Protecting Against Chemical Terrorism**

  The Agency for Toxic Substances and Disease Registry (ATSDR) developed a risk management methodology to "assist local public health and safety officials in analyzing, mitigating and preventing [chemical terrorism]." This procedure consists of ten steps, mainly focused on the RMSEF's scoping, strategy, and action steps.

- **Transportation Loss Prevention & Security Council Security Survey**

  Unlike the security risk management protocols described above, this procedure is intended for use by individual companies wishing to enhance the physical security of their property. This security survey consists of five elements similar to the RMSEF's scoping, knowledge of operations, and strategy steps.