Hazmat Transportation Risk Assessment

Risk Area	Risk Identification and Analysis (likelihood of occurring)				Risk Countermeasure (plan development item)
	Not at all likely	Some-what likely	Likely	Very likely	[____Include only those below that apply. Modify or delete those that do not reflect your operation. Add additional topics that are unique to your motor carrier.____]
Hazmat theft risks:					
At company facility	☐	☐	☐	☐	— Develop a site-specific security assessment and security plan for each location/terminal of the organization, unique to its layout, design, location, etc. — Develop procedures to segregate hazmat cargo in a separate and secure area that limits and controls employee access. — Communicate security procedures regarding restricted hazmat areas and sensitive/confidential records with all employees. — Conduct thorough background investigations (including criminal conviction history) on all current and prospective employees who will have access to hazardous materials or related paperwork. — Develop professional working relationship with local law enforcement agencies, including regional FBI office(s). — Have law enforcement conduct a facility risk assessment. — Conduct frequent, unscheduled facility security audits and inspections. — Periodically inventory the types and quantities of hazardous materials stored on site in order to recognize if a theft has occurred. — Put policies and procedures in place (unique to the operation and commodity) that reflect changes in the Homeland Security Advisory System, industry alerts, maritime MARSEC levels (if applicable), and trends/political climates. — [____Enter additional topics not listed____]
En route	☐	☐	☐	☐	— Develop and implement driver cargo security procedures and general driver security awareness training. — Develop effective and timely cargo theft reporting procedures. — Explore terminal-to-truck communication options. — Provide “worst case scenario” vehicle hijacking survival training to all drivers. — Develop professional working relationship with local law enforcement agencies, including regional state patrol and FBI office(s). — Review the safety rating, assessment, compliance audit and credit history, and ask for all security-related procedures before using any carrier for the purposes of transporting hazardous materials. — Verify that the prospective carrier has adequate security

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

					hiring and screening procedures in place. — Verify the identity of the motor carrier and/or driver prior to loading any hazardous material. — Develop communication procedures (terminal-to-truck), alternate routes, and other policies and procedures in the event the Department of Homeland Security (DHS) Advisory System is changed, industry alerts are posted, maritime MARSEC level is raised (if applicable), or trends/political climates change. — [____Enter additional topics not listed____]
Personnel security risks:					
All employees	☐	☐	☐	☐	— Identify, by job title of the senior management official, who is responsible for overall development and implementation of the security plan. — Identify security duties for each position or department that is responsible for implementing the plan or a portion of the plan and the process of notifying employees when specific elements of the security plan must be implemented. — Create thorough job descriptions, organizational charts, and reporting structures for decision-making. Determine who: creates and maintains policies and procedures; reports to whom about security concerns/incidents; and has access to which information. Generate this list for each location and relationships between locations and the home office. — Conduct thorough background investigations (including criminal conviction history) of all prospective and (periodically on) current employees who will have access to hazardous materials and/or related records and information. — Develop and communicate corporate security procedures regarding restricted hazmat areas and related records and information with all employees. — Include security training in company security objectives, organizational security structure, specific security procedures, specific security duties and responsibilities for each employee, and specific actions to be taken by each employee in the event of a security breach. — Conduct suspicious activity awareness training for all employees once every 3 years. — Conduct in-depth security training required under §172.704(a)(5) at least once every three years, or within 90 days of implementation when the security plan for which training is required is revised during the three-year recurrent training cycle. — Conduct regular security training meetings for all employees. — Review current trends and threat conditions. — Train employees on their roles, communication, and other details associated with a change in the DHS or maritime/MARSEC security threat levels. — [____Enter additional topics not listed____]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Driver applicants	☐	☐	☐	☐	— Develop and maintain adequate driver qualification and screening hiring standards for new drivers. — Conduct thorough background investigations (including criminal conviction history) of all prospective drivers who will transport hazardous materials. — Verify all information provided by driver applicants (as listed on the original driver's application). — [____Enter additional topics not listed____]
Existing drivers	☐	☐	☐	☐	— Ensure all drivers receive adequate personal safety and cargo security training. — Develop and implement procedures that ensure the security and confidentiality of all driver-related files and documents including DQ files, Driver Investigation History files, D&A files, personnel records, records of duty status, payroll records, driver settlement statements, etc. — Ensure all drivers designated to transport hazardous materials remain qualified to operate a commercial motor vehicle. — Conduct periodic and random criminal investigations on existing drivers. — Explore terminal-to-truck communication options. — Ensure drivers are trained in communication procedures (terminal-to-truck), alternate routes, and other policies and procedures in the event the DHS Advisory System is changed, industry alerts are posted, maritime MARSEC level (if applicable) is raised, or trends/political climates change. — [____Enter additional topics not listed____]
Leased drivers	☐	☐	☐	☐	— Conduct a thorough background investigation on all leasing companies used including a credit check and review of client references. — Contact leasing company and review and verify the DQ files of all drivers to be used. — Ensure that all leased drivers designated to transport hazardous materials remain qualified to operating a commercial motor vehicle.
Unauthorized access security risks:					
Operations	☐	☐	☐	☐	— Limit and control all facility access points, and especially those leading to hazardous materials and critical/sensitive records storage areas. — Establish procedures that prohibit unauthorized access into physical facilities, and especially areas that contain hazardous materials. — Conduct frequent and unscheduled security audits and inspections of all areas of the operation. — Establish partnerships with local law enforcement officials, emergency responders, and other public safety agencies. — Have local law enforcement conduct a facility risk assessment. — Develop a written policy that prohibits any employee from

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

					sharing or leaving unattended sensitive or critical information. — Develop a written email and electronic documents policy that defines exactly what information can and cannot be sent out electronically. — Require all employees to display identification cards or badges when on company premises. — Maintain records of all security-related incidents to help identify trends and potential vulnerabilities. — Report all suspicious activity or individuals to local law enforcement officials or the FBI. — Complete a site-specific security assessment and security plan for each location of the organization, unique to its layout, design, location, etc. — Put policies and procedures in place (unique to the operation and commodity) that reflect changes in the Homeland Security Advisory System, industry alerts, maritime MARSEC level (if applicable), and trends/political climates. — Create policies and procedures on distributing information related to hazmat shipments, including information to business partners. — [____Enter additional topics not listed____]
Visitors, vendors, and suppliers	☐	☐	☐	☐	— Restrict general access to all company facilities to a single point of entry. — Require all visitors to identify themselves with a photo ID and to register (sign in). — Upgrade security procedures for all vendors and suppliers to the company. — Restrict access when the Homeland Security Advisory System raises, industry alerts are issued, maritime MARSEC level is raised (if applicable), or trends/political climates change. These controls should be unique to the operation, commodity, and type of vendor or visitor. — [____Enter additional topics not listed____]
Yard security	☐	☐	☐	☐	— Secure hazardous materials in locked buildings or fenced storage areas. Implement a sign-in/out system for access to these areas. — Secure all valves, manways, and other fixtures on transportation equipment when not in use (tank-trailer operations). Lock and seal all trailers when not in use (all other motor carrier operations). — Use tamper-resistant or tamper-evident seals and heavy duty locks on all cargo trailers. — Ensure the yard and parking areas have adequate security lighting. — Conduct frequent security inspections of the yard that includes staged equipment. — Ensure all access points (doors and windows) are locked and secured from the inside when not in use. — Create additional yard security policies and procedures when the Homeland Security Advisory System raises, industry

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

					alerts are posted, maritime MARSEC level raises (if applicable), or trends/political climates change. — [____Enter additional topics not listed____]
En route security risks:					
Hazmat drivers	☐	☐	☐	☐	— Train driver on proper security pre-trip inspection procedures, including looking for any foreign objects or materials. — Train drivers in proper cargo pick up security procedures including the need to produce photo identification to responsible shipping personnel. — Train drivers to maintain regular communication with their dispatcher/terminal. — Train drivers to look out for any suspicious activity — especially when leaving any shipper. — Train driver to never discuss any load-related information with any unauthorized or unidentified individuals outside the company including load content, pick-up and delivery schedules, and routing information. — Train drivers in security parking, stopping, and breaking procedures. — Train drivers to re-inspect their vehicle after every stop. — Train drivers on the organization's security protocols when the Homeland Security Advisory System raises, industry alerts are posted, maritime MARSEC levels raised (if applicable), or trends/political climates change. — [____Enter additional topics not listed____]
Hazmat operations personnel	☐	☐	☐	☐	— Avoid assigning any hazmat load to new drivers for at least the first six months of employment. — Develop and implement en route communication/check in procedures for all hazmat drivers. — Work with customers to expedite deliveries and reduce transit/down time while drivers are en route. — Conduct frequent yard checks — especially during off-hours, and evenings and weekends. — Establish timely and standard procedures for reporting suspicious activity and cargo theft incidents. — Create even more of a stringent "need-to-know" scope than usual in reference to hazmat-related information when the Homeland Security Advisory System raises, industry alerts are posted, maritime MARSEC level is raised (if applicable), or trends/political climates change. — [____Enter additional topics not listed____]

Assessment Completed by: _____ Facility Location:_____

Date: _____ Next Review Date (within 12 months):_____

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.