

HAZARDOUS MATERIALS REGULATIONS

table of contents

49 CFR Part 15

49 CFR Part 172.800

49 CFR Part 172 Subpart C through Subpart G

49 CFR Part 172 Subpart H

49 CFR Part 177 Subpart A

49 CFR Part 383 Subpart B

49 CFR Part 383 Subpart G

49 CFR Part 383 Subpart I

49 CFR Part 391 Subpart C

49 CFR Part 392 Subpart G

49 CFR Part 397 Subpart A

49 CFR Part 397 Subparts C and D

49 CFR Parts 1570 and 1572

49 CFR Part 1572

Risk Management Self-Evaluation Framework (RMSEF)

A Guide to Developing an Effective Security Plan for the Highway
Transportation of Hazardous Materials

(c) *Initial and recurrent training*—(1) *Initial training.* A new hazmat employee, or a hazmat employee who changes job functions may perform those functions prior to the completion of training provided—

(i) The employee performs those functions under the direct supervision of a properly trained and knowledgeable hazmat employee; and

(ii) The training is completed within 90 days after employment or a change in job function.

(2) *Recurrent training.* A hazmat employee shall receive the training required by this subpart at least once every three years.

(3) *Relevant Training.* Relevant training received from a previous employer or other source may be used to satisfy the requirements of this subpart provided a current record of training is obtained from hazmat employees' previous employer.

(4) *Compliance.* Each hazmat employer is responsible for compliance with the requirements of this subchapter regardless of whether the training required by this subpart has been completed.

(d) *Recordkeeping.* A record of current training, inclusive of the preceding three years, in accordance with this section shall be created and retained by each hazmat employer for as long as that employee is employed by that employer as a hazmat employee and for 90 days thereafter. The record shall include:

(1) The hazmat employee's name;

(2) The most recent training completion date of the hazmat employee's training;

(3) A description, copy, or the location of the training materials used to meet the requirements in paragraph (a) of this section;

(4) The name and address of the person providing the training; and

(5) Certification that the hazmat employee has been trained and tested, as required by this subpart.

(e) *Limitation.* A hazmat employee who repairs, modifies, reconditions, or tests packagings as qualified for use in the transportation of hazardous materials, and who does not perform any other function subject to the requirements of this subchapter, is not subject

to the safety training requirement of paragraph (a)(3) of this section.

[Amdt. 172-126, 57 FR 20952, May 15, 1992, as amended by Amdt. 172-126, 58 FR 5851, Jan. 22, 1993; Amdt. 172-145, 60 FR 49110, Sept. 21, 1995; Amdt. 172-149, 61 FR 27173, May 30, 1996; 65 FR 50460, Aug. 18, 2000; 68 FR 14521, Mar. 25, 2003]

Subpart I—Security Plans

SOURCE: 68 FR 14521, Mar. 25, 2003, unless otherwise noted.

§ 172.800 Purpose and applicability.

(a) *Purpose.* This subpart prescribes requirements for development and implementation of plans to address security risks related to the transportation of hazardous materials in commerce.

(b) *Applicability.* By September 25, 2003, each person who offers for transportation in commerce or transports in commerce one or more of the following hazardous materials must develop and adhere to a security plan for hazardous materials that conforms to the requirements of this subpart:

(1) A highway route-controlled quantity of a Class 7 (radioactive) material, as defined in §173.403 of this subchapter, in a motor vehicle, rail car, or freight container;

(2) More than 25 kg (55 pounds) of a Division 1.1, 1.2, or 1.3 (explosive) material in a motor vehicle, rail car, or freight container;

(3) More than one L (1.06 qt) per package of a material poisonous by inhalation, as defined in §171.8 of this subchapter, that meets the criteria for Hazard Zone A, as specified in §§173.116(a) or 173.133(a) of this subchapter;

(4) A shipment of a quantity of hazardous materials in a bulk packaging having a capacity equal to or greater than 13,248 L (3,500 gallons) for liquids or gases or more than 13.24 cubic meters (468 cubic feet) for solids;

(5) A shipment in other than a bulk packaging of 2,268 kg (5,000 pounds) gross weight or more of one class of hazardous materials for which placarding of a vehicle, rail car, or freight container is required for that class under the provisions of subpart F of this part;

§ 172.802

(6) A select agent or toxin regulated by the Centers for Disease Control and Prevention under 42 CFR part 73; or

(7) A quantity of hazardous material that requires placarding under the provisions of subpart F of this part.

§ 172.802 Components of a security plan.

(a) The security plan must include an assessment of possible transportation security risks for shipments of the hazardous materials listed in § 172.800 and appropriate measures to address the assessed risks. Specific measures put into place by the plan may vary commensurate with the level of threat at a particular time. At a minimum, a security plan must include the following elements:

(1) *Personnel security.* Measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan. Such confirmation system must be consistent with applicable Federal and State laws and requirements concerning employment practices and individual privacy.

(2) *Unauthorized access.* Measures to address the assessed risk that unauthorized persons may gain access to the hazardous materials covered by the security plan or transport conveyances being prepared for transportation of the hazardous materials covered by the security plan.

(3) *En route security.* Measures to address the assessed security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement.

(b) The security plan must be in writing and must be retained for as long as it remains in effect. Copies of the security plan, or portions thereof, must be available to the employees who are responsible for implementing it, consistent with personnel security clearance or background investigation re-

49 CFR Ch. I (10–1–05 Edition)

strictions and a demonstrated need to know. The security plan must be revised and updated as necessary to reflect changing circumstances. When the security plan is updated or revised, all copies of the plan must be maintained as of the date of the most recent revision.

§ 172.804 Relationship to other Federal requirements.

To avoid unnecessary duplication of security requirements, security plans that conform to regulations, standards, protocols, or guidelines issued by other Federal agencies, international organizations, or industry organizations may be used to satisfy the requirements in this subpart, provided such security plans address the requirements specified in this subpart.

APPENDIX A TO PART 172—OFFICE OF HAZARDOUS MATERIALS TRANSPORTATION COLOR TOLERANCE CHARTS AND TABLES

The following are Munsell notations and Commission Internationale de L'Eclairage (CIE) coordinates which describe the Office of Hazardous Materials Transportation Label and Placard Color Tolerance Charts in tables 1 and 2, and the CIE coordinates for the color tolerances specified in table 3. Central colors and tolerances described in table 2 approximate those described in table 1 while allowing for differences in production methods and materials used to manufacture labels and placards surfaced with printing inks. Primarily, the color charts based on table 1 are for label or placard colors applied as opaque coatings such as paint, enamel or plastic, whereas color charts based on table 2 are intended for use with labels and placards surfaced only with inks.

For labels printed directly on packaging surfaces, table 3 may be used, although compliance with either table 1 or table 2 is sufficient. However, if visual reference indicates that the colors of labels printed directly on package surfaces are outside the table 1 or 2 tolerances, a spectrophotometer or other instrumentation may be required to insure compliance with table 3.

TABLE 1—SPECIFICATIONS FOR COLOR TOLERANCE CHARTS FOR USE WITH LABELS AND PLACARDS SURFACED WITH PAINT, LACQUER, ENAMEL, PLASTIC, OTHER OPAQUE COATINGS, OR INK¹

Color	Munsell notations	CIE data for source C		
		Y	x	y
Red:				
Central color	7.5R 4.0/14	12.00	.5959	.3269
Orange	8.5R 4.0/14	12.00	.6037	.3389
Purple and vivid	6.5R 4.0/14	12.00	.5869	.3184
Grayish	7.5R 4.0/12	12.00	.5603	.3321
Vivid	7.5R 4.0/16	12.00	.6290	.3192
Light	7.5R 4.5/14	15.57	.5775	.3320
Dark	7.5R 3.5/14	09.00	.6226	.3141
Orange:				
Central color	5.OYR 6.0/15	30.05	.5510	.4214
Yellow and Grayish	6.25YR 6.0/15	30.05	.5452	.4329
Red and vivid	3.75YR 6.0/15	30.05	.5552	.4091
Grayish	5.OYR 6.0/13	30.05	.5311	.4154
Vivid	5.OYR 6.0/16	30.05	.5597	.4239
Light	5.OYR 6.5/15	36.20	.5427	.4206
Dark	5.OYR 5.5/15	24.58	.5606	.4218
Yellow:				
Central color	5.OY 8.0/12	59.10	.4562	.4788
Green	6.5Y 8.0/12	59.10	.4498	.4865
Orange and vivid	3.5Y 8.0/12	59.10	.4632	.4669
Grayish	5.OY 8.0/10	59.10	.4376	.4601
Vivid	5.OY 8.0/14	59.10	.4699	.4920
Light	5.OY 8.5/12	68.40	.4508	.4754
Dark	5.OY 7.5/12	50.68	.4620	.4823
Green:				
Central color	7.5G 4.0/9	12.00	.2111	.4121
Bluish	0.5BG 4.0/9	12.00	.1974	.3809
Green-yellow	5.0G 4.0/9	12.00	.2237	.4399
Grayish A	7.5G 4.0/7	12.00	.2350	.3922
Grayish B ²	7.5G 4.0/6	12.00	.2467	.3822
Vivid	7.5G 4.0/11	12.00	.1848	.4319
Light	7.5G 4.5/9	15.57	.2204	.4060
Dark	7.5G 3.5/9	09.00	.2027	.4163
Blue:				
Central color	2.5PB 3.5/10	09.00	.1691	.1744
Purple	4.5PB 3.5/10	09.00	.1796	.1711
Green and vivid	10.0B 3.5/10	09.00	.1557	.1815
Grayish	2.5PB 3.5/8	09.00	.1888	.1964
Vivid	2.5PB 3.5/12	09.00	.1516	.1547
Light	2.5PB 4.0/10	12.00	.1805	.1888
Dark	2.5PB 3.0/10	06.55	.1576	.1600
Purple:				
Central color	10.0P 4.5/10	15.57	.3307	.2245
Reddish purple	2.5RP 4.5/10	15.57	.3584	.2377
Blue purple	7.5P 4.5/10	15.57	.3068	.2145
Reddish gray	10.0P 4.5/8	15.57	.3280	.2391
Gray ²	10.0P 4.5/6.5	15.57	.3254	.2519
Vivid	10.0P 4.5/12	15.57	.3333	.2101
Light	10.0P 5.0/10	19.77	.3308	.2328
Dark	10.0P 4.0/10	12.00	.3306	.2162

¹ Maximum chroma is not limited.
² For the colors green and purple, the minimum saturation (chroma) limits for porcelain enamel on metal are lower than for most other surface coatings. Therefore, the minimum chroma limits of these two colors as displayed on the Charts for comparison to porcelain enamel on metal is low, as shown for green (grayish B) and purple (gray).
 NOTE: CIE=Commission Internationale de L'Eclairage.

TABLE 2—SPECIFICATIONS FOR COLOR TOLERANCE CHARTS FOR USE WITH LABELS AND PLACARDS SURFACED WITH INK

Color/series	Munsell notation	CIE data for source C		
		Y	x	y
Red:				
Central series:				
Central color	6.8R 4.47/12.8	15.34	.5510	.3286
Grayish	7.2R 4.72/12.2	17.37	.5368	.3348
Purple	6.4R 4.49/12.7	15.52	.5442	.3258
Purple and vivid	6.1R 4.33/13.1	14.25	.5529	.3209

TABLE 2—SPECIFICATIONS FOR COLOR TOLERANCE CHARTS FOR USE WITH LABELS AND PLACARDS SURFACED WITH INK—Continued

Color/series	Munsell notation	CIE data for source C		
		Y	x	y
Vivid	6.7R 4.29/13.2	13.99	.5617	.3253
Orange	7.3R 4.47/12.8	15.34	.5572	.3331
Orange and grayish	7.65R 4.70/12.4	17.20	.5438	.3382
Light series:				
Light	7.0R 4.72/13.2	17.32	.5511	.3322
Light and orange	7.4R 4.96/12.6	19.38	.5365	.3392
Light and purple	6.6R 4.79/12.9	17.94	.5397	.3289
Dark series:				
Dark A	6.7R 4.19/12.5	13.30	.5566	.3265
Dark B	7.0R 4.25/12.35	13.72	.5522	.3294
Dark and purple	7.5R 4.23/12.4	13.58	.5577	.3329
Orange:				
Central series:				
Central color	5.0YR 6.10/12.15	31.27	.5193	.4117
Yellow and grayish A	5.8YR 6.22/11.7	32.69	.5114	.4155
Yellow and grayish B	6.1YR 6.26/11.85	33.20	.5109	.4190
Vivid	5.1YR 6.07/12.3	30.86	.5226	.4134
Red and vivid A	3.9YR 5.87/12.75	28.53	.5318	.4038
Red and vivid B	3.6YR 5.91/12.6	29.05	.5291	.4021
Grayish	4.9YR 6.10/11.9	31.22	.5170	.4089
Light series:				
Light and vivid A	5.8YR 6.78/12.7	39.94	.5120	.4177
Light and yellow	6.0YR 6.80/12.8	40.20	.5135	.4198
Light and vivid B	4.9YR 6.60/12.9	37.47	.5216	.4126
Dark series:				
Dark and yellow	5.8YR 5.98/11.0	29.87	.5052	.4132
Dark A	5.1YR 5.80/11.1	27.80	.5127	.4094
Dark B	5.0YR 5.80/11.0	27.67	.5109	.4068
Yellow:				
Central series:				
Central color	4.3Y 7.87/10.3	56.81	.4445	.4589
Vivid A	4.5Y 7.82/10.8	55.92	.4503	.4658
Vivid B	3.3Y 7.72/11.35	54.24	.4612	.4624
Vivid and orange	3.2Y 7.72/10.8	54.25	.4576	.4572
Grayish A	4.1Y 7.95/9.7	58.18	.4380	.4516
Grayish B	5.1Y 8.06/9.05	60.12	.4272	.4508
Green-yellow	5.2Y 7.97/9.9	58.53	.4356	.4605
Light series:				
Light	5.4Y 8.59/10.5	70.19	.4351	.4628
Light and green-yellow	5.4Y 8.56/11.2	69.59	.4414	.4692
Light and vivid	4.4Y 8.45/11.4	67.42	.4490	.4662
Dark series:				
Dark and green-yellow	4.4Y 7.57/9.7	51.82	.4423	.4562
Dark and orange A	3.4Y 7.39/10.4	48.86	.4584	.4590
Dark and orange B	3.5Y 7.41/10.0	49.20	.4517	.4544
Green:				
Central series:				
Central color	9.75G 4.26/7.75	13.80	.2214	.3791
Grayish	10G 4.46/7.5	15.25	.2263	.3742
Blue A	1.4BG 4.20/7.4	13.36	.2151	.3625
Blue B	1.0BG 4.09/7.75	12.60	.2109	.3685
Vivid	8.4G 4.09/8.05	12.59	.2183	.3954
Vivid green-yellow	7.0G 4.23/8.0	13.54	.2292	.4045
Green-yellow	7.85G 4.46/7.7	15.23	.2313	.3914
Light series:				
Light and vivid	9.5G 4.45/8.8	15.21	.2141	.3863
Light and blue	0.2BG 4.31/8.8	14.12	.2069	.3814
Light and green-yellow	8.3G 4.29/9.05	14.01	.2119	.4006
Dark series:				
Dark and green-yellow	7.1G 4.08/7.1	12.55	.2354	.3972
Dark and grayish	9.5G 4.11/6.9	12.70	.2282	.3764
Dark	8.5G 3.97/7.2	11.78	.2269	.3874
Blue:				
Central series:				
Central color	3.5PB 3.94/9.7	11.58	.1885	.1911
Green and grayish A	2.0PB 4.35/8.7	14.41	.1962	.2099
Green and grayish B	1.7PB 4.22/9.0	13.50	.1898	.2053
Vivid	2.9PB 3.81/9.7	10.78	.1814	.1852
Purple and vivid A	4.7PB 3.53/10.0	9.15	.1817	.1727

TABLE 2—SPECIFICATIONS FOR COLOR TOLERANCE CHARTS FOR USE WITH LABELS AND PLACARDS SURFACED WITH INK—Continued

Color/series	Munsell notation	CIE data for source C		
		Y	x	y
Purple and vivid B	5.0PB 3.71/9.9	10.20	.1888	.1788
Grayish	3.75PB 4.03/9.1	12.17	.1943	.1961
Light series:				
Light and green A	1.7PB 4.32/9.2	14.22	.1904	.2056
Light and green B	1.5PB 4.11/9.6	12.72	.1815	.1971
Light and vivid	3.2PB 3.95/10.05	11.70	.1831	.1868
Dark series:				
Dark and grayish	3.9PB 4.01/8.7	12.04	.1982	.1992
Dark and purple A	4.8PB 3.67/9.3	9.95	.1918	.1831
Dark and purple B	5.2PB 3.80/9.05	10.76	.1985	.1885
Purple:				
Central series:				
Central color	9.5P 4.71/11.3	17.25	.3274	.2165
Red	1.0RP 5.31/10.8	22.70	.3404	.2354
Red and vivid A	1.4RP 5.00/11.9	19.78	.3500	.2274
Red and vivid B	0.2RP 4.39/12.5	14.70	.3365	.2059
Vivid	8.0P 4.04/12.0	12.23	.3098	.1916
Blue	7.0P 4.39/10.8	14.71	.3007	.2037
Grayish	8.8P 5.00/10.3	19.73	.3191	.2251
Light series:				
Light and red A	0.85RP 5.56/11.1	25.18	.3387	.2356
Light and red B	1.1RP 5.27/12.3	22.27	.3460	.2276
Light and vivid	9.2P 4.94/11.95	19.24	.3247	.2163
Dark series:				
Dark and grayish	9.6P 4.70/10.9	17.19	.3283	.2204
Dark and vivid	8.4P 4.05/11.6	12.35	.3144	.1970
Dark and blue	7.5P 4.32/10.5	14.19	.3059	.2078

TABLE 3—SPECIFICATION FOR COLORS FOR USE WITH LABELS PRINTED ON PACKAGINGS SURFACES

CIE data for source C	Red	Orange	Yellow	Green	Blue	Purple
x424	.460	.417	.228	.200	.377
y306	.370	.392	.354	.175	.205
x571	.543	.490	.310	.255	.377
y306	.400	.442	.354	.250	.284
x424	.445	.390	.228	.177	.342
y350	.395	.430	.403	.194	.205
x571	.504	.440	.310	.230	.342
y350	.430	.492	.403	.267	.284
Y (high)	23.0	41.6	72.6	20.6	15.9	21.2
Y (low)	7.7	19.5	29.1	7.4	6.5	8.2

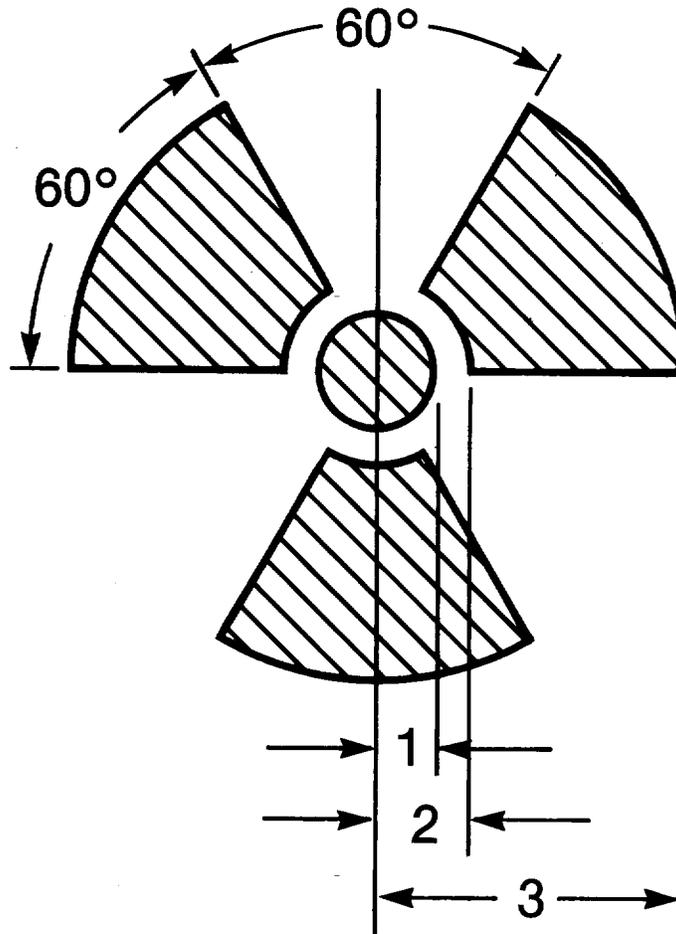
[Amdt. 172-50, 44 FR 9757, Feb. 15, 1979; Amdt. 172-50, 44 FR 10984, Feb. 26, 1979, as amended by Amdt. 172-50, 44 FR 22467, Apr. 16, 1979; 50 FR 45731, Nov. 1, 1985; Amdt. 172-127, 59 FR 49133, Sept. 26, 1994]

APPENDIX B TO PART 172—TREFOIL SYMBOL

1. Except as provided in paragraph 2 of this appendix, the trefoil symbol required for RADIOACTIVE labels and placards and required to be marked on certain packages of Class 7

materials must conform to the design and size requirements of this appendix.

2. RADIOACTIVE labels and placards that were printed prior to April 1, 1996, in conformance with the requirements of this subchapter in effect on March 30, 1996, may continue to be used.

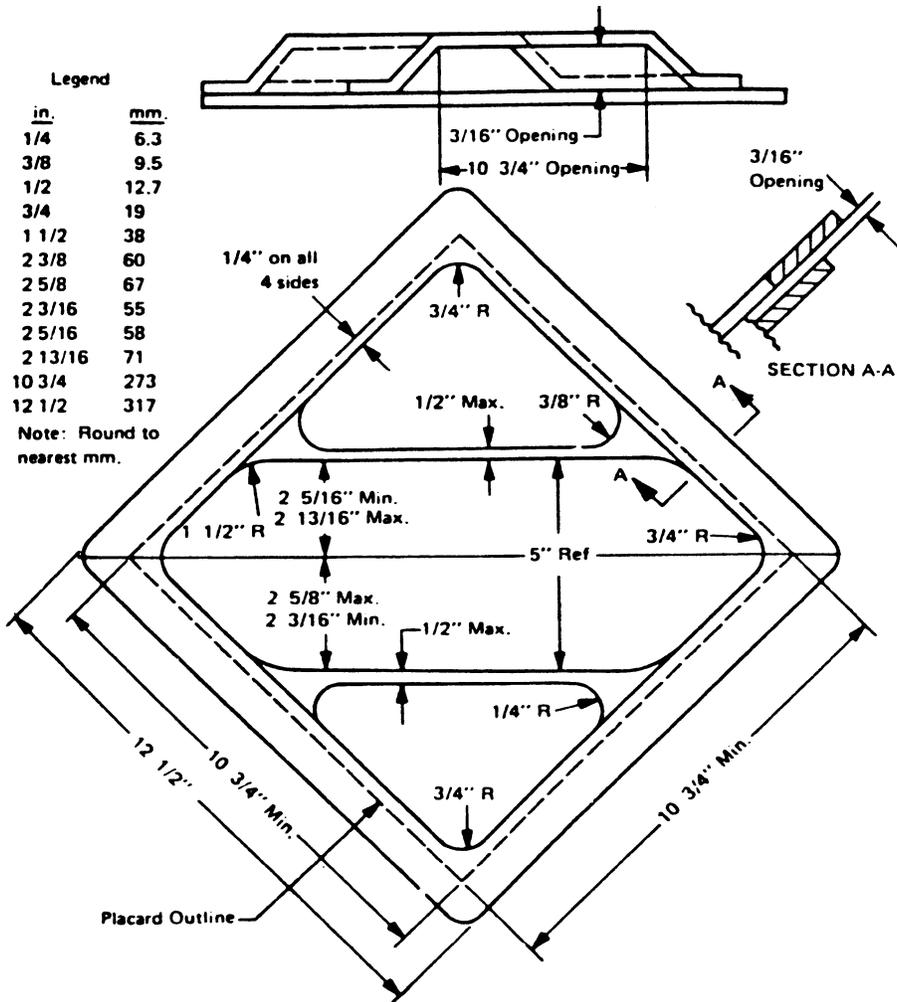


1=Radius of Circle—
Minimum dimensions
4 mm (0.16 inch) for markings and labels
12.5 mm (0.5 inch) for placards
2=1½ Radii

3=5 radii for markings and labels
4½ radii for placards.

[60 FR 50306, Sept. 28, 1995, as amended by
172-143, 61 FR 20750, May 8, 1996]

APPENDIX C TO PART 172—DIMENSIONAL SPECIFICATIONS FOR RECOMMENDED PLACARD HOLDER



PART 173—SHIPPERS—GENERAL REQUIREMENTS FOR SHIPMENTS AND PACKAGINGS

Subpart A—General

- Sec.
 173.1 Purpose and scope.
 173.2 Hazardous materials classes and index to hazard class definitions.
 173.2a Classification of a material having more than one hazard.

- 173.3 Packaging and exceptions.
 173.4 Small quantity exceptions.
 173.5 Agricultural operations.
 173.5a Oilfield service vehicles and mechanical displacement meter provers.
 173.6 Materials of trade exceptions.
 173.7 U.S. Government material.
 173.8 Exceptions for non-specification packagings used in intrastate transportation.
 173.9 Transport vehicles or freight containers containing lading which has been fumigated.
 173.10 Tank car shipments.

§ 172.200

plastic bags, plastic film bags, textile bags, paper bags, IBCs and bulk packagings.

W41 When offered for transportation by water, this material must be packaged in bales and be securely and tightly bound with rope, wire or similar means.

[Amdt. 172-123, 55 FR 52582, Dec. 21, 1990]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 172.102, see the List of CFR Sections Affected which appears in the Finding Aids section of the printed volume and on GPO Access.

Subpart C—Shipping Papers

§ 172.200 Applicability.

(a) *Description of hazardous materials required.* Except as otherwise provided in this subpart, each person who offers a hazardous material for transportation shall describe the hazardous material on the shipping paper in the manner required by this subpart.

(b) This subpart does not apply to any material, other than a hazardous substance, hazardous waste or marine pollutant, that is—

(1) Identified by the letter “A” in column 1 of the § 172.101 table, except when the material is offered or intended for transportation by air; or

(2) Identified by the letter “W” in column 1 of the § 172.101 table, except when the material is offered or intended for transportation by water; or

(3) An ORM-D, except when the material is offered or intended for transportation by air.

[Amdt. 172-29A, 41 FR 40677, Sept. 20, 1976, as amended by Amdt. 172-58, 45 FR 34697, May 22, 1980; Amdt. 172-74, 47 FR 43065, Sept. 30, 1982; Amdt. 172-112, 53 FR 17160, May 13, 1988; Amdt. 172-127, 57 FR 52938, Nov. 5, 1992]

§ 172.201 Preparation and retention of shipping papers.

(a) *Contents.* When a description of hazardous material is required to be included on a shipping paper, that description must conform to the following requirements:

(1) When a hazardous material and a material not subject to the requirements of this subchapter are described on the same shipping paper, the hazardous material description entries required by § 172.202 and those additional entries that may be required by § 172.203:

49 CFR Ch. I (10-1-05 Edition)

(i) Must be entered first, or

(ii) Must be entered in a color that clearly contrasts with any description on the shipping paper of a material not subject to the requirements of this subchapter, except that a description on a reproduction of a shipping paper may be highlighted, rather than printed, in a contrasting color (the provisions of this paragraph apply only to the basic description required by § 172.202(a)(1), (2), (3), and (4)), or

(iii) Must be identified by the entry of an “X” placed before the proper shipping name in a column captioned “HM.” (The “X” may be replaced by “RQ,” if appropriate.)

(2) The required shipping description on a shipping paper and all copies thereof used for transportation purposes, must be legible and printed (manually or mechanically) in English.

(3) Unless it is specifically authorized or required in this subchapter, the required shipping description may not contain any code or abbreviation.

(4) A shipping paper may contain additional information concerning the material provided the information is not inconsistent with the required description. Unless otherwise permitted or required by this subpart, additional information must be placed after the basic description required by § 172.202(a).

(b) [Reserved]

(c) *Continuation page.* A shipping paper may consist of more than one page, if each page is consecutively numbered and the first page bears a notation specifying the total number of pages included in the shipping paper. For example, “Page 1 of 4 pages.”

(d) *Emergency response telephone number.* Except as provided in § 172.604(c), a shipping paper must contain an emergency response telephone number, as prescribed in subpart G of this part.

(e) Each person who provides a shipping paper must retain a copy of the shipping paper required by § 172.200(a), or an electronic image thereof, that is accessible at or through its principal place of business and must make the shipping paper available, upon request, to an authorized official of a Federal, State, or local government agency at reasonable times and locations. For a hazardous waste, the shipping paper

copy must be retained for three years after the material is accepted by the initial carrier. For all other hazardous materials, the shipping paper copy must be retained for 375 days after the material is accepted by the initial carrier. Each shipping paper copy must include the date of acceptance by the initial carrier, except that, for rail, vessel, or air shipments, the date on the shipment waybill, airbill, or bill of lading may be used in place of the date of acceptance by the initial carrier. A motor carrier (as defined in §390.5 of subchapter B of chapter III of subtitle B) using a shipping paper without change for multiple shipments of one or more hazardous materials having the same shipping name and identification number may retain a single copy of the shipping paper, instead of a copy for each shipment made, if the carrier also retains a record of each shipment made, to include shipping name, identification number, quantity transported, and date of shipment.

[Amdt. 172-29A, 41 FR 40677, Sept. 20, 1976]

EDITORIAL NOTE: FOR FEDERAL REGISTER citations affecting §172.201, see the List of CFR Sections Affected which appears in the Finding Aids section of the printed volume and on GPO Access.

§ 172.202 Description of hazardous material on shipping papers.

(a) The shipping description of a hazardous material on the shipping paper must include:

(1) The proper shipping name prescribed for the material in column 2 of the §172.101 table;

(2) The hazard class or division number prescribed for the material, as shown in Column (3) of the §172.101 Table. Except for combustible liquids, the subsidiary hazard class(es) or subsidiary division number(s) must be entered in parentheses immediately following the primary hazard class or division number.

In addition—

(i) The words “Class” or “Division” may be included preceding the primary and subsidiary hazard class or division numbers.

(ii) The hazard class need not be included for the entry “Combustible liquid, n.o.s.”.

(iii) For domestic shipments, primary and subsidiary hazard class or division names may be entered following the numerical hazard class or division, or following the basic description.

(3) The identification number prescribed for the material as shown in column 4 of the §172.101 table;

(4) The packing group in Roman numerals, as designated for the hazardous material in Column 5 of the §172.101 Table. Class 1 (explosives) materials, self-reactive substances, organic peroxides and entries that are not assigned a packing group are excepted from this requirement. The packing group may be preceded by the letters “PG” (for example, “PG II”); and

(5) The total quantity of hazardous materials covered by the description must be indicated (by mass or volume, or by activity for Class 7 materials) and must include an indication of the applicable unit of measurement. For example, “200 kgs.” or “50 L.” The following provisions also apply:

(i) For Class 1 materials, the quantity must be the net explosive mass. For an explosive that is an article, such as Cartridges, small arms, the net explosive mass may be expressed in terms of the net mass of either the article or the explosive materials contained in the article.

(ii) For hazardous materials in salvage packaging, an estimate of the total quantity is acceptable.

(iii) The following are excepted from the requirements of paragraph (a)(5) of this section:

(A) Bulk packages, provided some indication of the total quantity is shown, for example, “1 cargo tank” or “2 IBCs.”

(B) Cylinders, provided some indication of the total quantity is shown, for example, “10 cylinders”.

(C) Packages containing only residue.

(6) The number and type of packages must be indicated. The type of packages must be indicated by description of the package (for example, “12 drums”). Indication of the packaging specification number (“1H1”) may be included in the description of the package (for example, “12 1H1 drums” or “12 drums (UN 1A1).” Abbreviations may be used for indicating packaging types (for example, “cyl.” for “cylinder”)

§ 172.203

49 CFR Ch. I (10–1–05 Edition)

provided the abbreviations are commonly accepted and recognizable.

(b) Except as provided in this subpart, the basic description specified in paragraphs (a)(1), (2), (3) and (4) of this section must be shown in sequence with no additional information interspersed. For example, “Cyclobutyl chloroformate, 6.1, (8,3), UN2744, PG II”. Alternatively, the basic description may be shown with the identification (ID) number listed first. For example, “UN2744, Cyclobutyl chloroformate, 6.1, (8, 3), PG II.”

(c) The total quantity of the material covered by one description must appear before or after, or both before and after, the description required and authorized by this subpart. The type of packaging and destination marks may be entered in any appropriate manner before or after the basic description. Abbreviations may be used to express units of measurement and types of packagings.

(d) Technical and chemical group names may be entered in parentheses between the proper shipping name and hazard class or following the basic description. An appropriate modifier, such as “contains” or “containing,” and/or the percentage of the technical constituent may also be used. For example: “Flammable liquids, n.o.s. (contains Xylene and Benzene), 3, UN 1993, II”.

(e) Except for those materials in the UN Recommendations, the ICAO Technical Instructions, or the IMDG Code (IBR, see §171.7 of this subchapter), a material that is not a hazardous material according to this subchapter may not be offered for transportation or transported when its description on a shipping paper includes a hazard class or an identification number specified in the §172.101 Table.

[Amdt. 172–101, 45 FR 74665, Nov. 10, 1980, as amended by Amdt. 172–103, 51 FR 5970, Feb. 18, 1986; Amdt. 172–123, 55 FR 52589, Dec. 21, 1990; 56 FR 66252, Dec. 20, 1991; Amdt. 172–127, 57 FR 52938, Nov. 5, 1992; Amdt. 172–130, 58 FR 51531, Oct. 1, 1993; 66 FR 33425, June 21, 2001; 68 FR 45030, July 31, 2003; 68 FR 75741, Dec. 31, 2003; 69 FR 34611, June 22, 2004; 69 FR 54046, Sept. 7, 2004; 69 FR 76153, Dec. 20, 2004; 70 FR 34397, June 14, 2005]

§ 172.203 Additional description requirements.

(a) *Exemptions.* Each shipping paper issued in connection with a shipment made under an exemption must bear the notation “DOT-E” followed by the exemption number assigned and so located that the notation is clearly associated with the description to which the exemption applies.

(b) *Limited quantities.* The description for a material offered for transportation as “limited quantity,” as authorized by this subchapter, must include the words “Limited Quantity” or “Ltd Qty” following the basic description.

(c) *Hazardous substances.* (1) Except for Class 7 (radioactive) materials described in accordance with paragraph (d) of this section, if the proper shipping name for a material that is a hazardous substance does not identify the hazardous substance by name, the name of the hazardous substance must be entered in parentheses in association with the basic description. If the material contains two or more hazardous substances, at least two hazardous substances, including the two with the lowest reportable quantities (RQs), must be identified. For a hazardous waste, the waste code (e.g., D001), if appropriate, may be used to identify the hazardous substance.

(2) The letters “RQ” shall be entered on the shipping paper either before or after, the basic description required by §172.202 for each hazardous substance (see definition in §171.8 of this subchapter). For example: “RQ, Allyl alcohol, 6.1, UN 1098, I”; or “Environmentally hazardous substance, solid, n.o.s., 9, UN 3077, III, RQ (Adipic acid)”.

(d) *Radioactive material.* The description for a shipment of a Class 7 (radioactive) material must include the following additional entries as appropriate:

(1) The name of each radionuclide in the Class 7 (radioactive) material that is listed in §173.435 of this subchapter. For mixtures of radionuclides, the radionuclides that must be shown must be determined in accordance with §173.433(g) of this subchapter. Abbreviations, e.g., “⁹⁹Mo,” are authorized.

(2) A description of the physical and chemical form of the material, if the

material is not in special form (generic chemical description is acceptable for chemical form).

(3) The activity contained in each package of the shipment in terms of the appropriate SI units (*e.g.*, Becquerels (Bq), Terabecquerels (TBq), etc.). The activity may also be stated in appropriate customary units (Curies (Ci), milliCuries (mCi), microCuries (uCi), etc.) in parentheses following the SI units. Abbreviations are authorized. Except for plutonium-239 and plutonium-241, the weight in grams or kilograms of fissile radionuclides may be inserted instead of activity units. For plutonium-239 and plutonium-241, the weight in grams of fissile radionuclides may be inserted in addition to the activity units.

(4) The category of label applied to each package in the shipment. For example: "RADIOACTIVE WHITE-I."

(5) The transport index assigned to each package in the shipment bearing RADIOACTIVE YELLOW-II or RADIOACTIVE YELLOW-III labels.

(6) For a package containing fissile Class 7 (radioactive) material:

(i) The words "Fissile Excepted" if the package is excepted pursuant to §173.453 of this subchapter; or otherwise

(ii) The criticality safety index for that package.

(7) For a package approved by the U.S. Department of Energy (DOE) or U.S. Nuclear Regulatory Commission (NRC), a notation of the package identification marking as prescribed in the applicable DOE or NRC approval (see §173.471 of the subchapter).

(8) For an export shipment or a shipment in a foreign made package, a notation of the package identification marking as prescribed in the applicable International Atomic Energy Agency (IAEA) Certificate of Competent Authority which has been issued for the package (see §173.473 of the subchapter).

(9) For a shipment required by this subchapter to be consigned as exclusive use:

(i) An indication that the shipment is consigned as exclusive use; or

(ii) If all the descriptions on the shipping paper are consigned as exclusive use, then the statement "Exclusive Use

Shipment" may be entered only once on the shipping paper in a clearly visible location.

(10) For the shipment of a package containing a highway route controlled quantity of Class 7 (radioactive) materials (see §173.403 of this subchapter) the words "Highway route controlled quantity" or "HRCQ" must be entered in association with the basic description.

(e) *Empty packagings.* (1) The description on the shipping paper for a packaging containing the residue of a hazardous material may include the words "RESIDUE: Last Contained * * *" in association with the basic description of the hazardous material last contained in the packaging.

(2) The description on the shipping paper for a tank car containing the residue of a hazardous material must include the phrase, "RESIDUE: LAST CONTAINED * * *" before the basic description.

(f) *Transportation by air.* A statement indicating that the shipment is within the limitations prescribed for either passenger and cargo aircraft or cargo aircraft only must be entered on the shipping paper.

(g) *Transportation by rail.* (1) A shipping paper prepared by a rail carrier for a rail car, freight container, transport vehicle or portable tank that contains hazardous materials must include the reporting mark and number when displayed on the rail car, freight container, transport vehicle or portable tank.

(2) The shipping paper for each DOT-113 tank car containing a Division 2.1 material or its residue must contain an appropriate notation, such as "DOT 113", and the statement "Do not hump or cut off car while in motion."

(3) When shipments of elevated temperature materials are transported under the exception permitted in §173.247(h)(3) of this subchapter, the shipping paper must contain an appropriate notation, such as "Maximum operating speed 15 mph."

(h) *Transportation by highway.* Following the basic description for a hazardous material in a Specification MC 330 or MC 331 cargo tank, there must be entered for—

(1) *Anhydrous ammonia.* (i) The words “0.2 PERCENT WATER” to indicate the suitability for shipping anhydrous ammonia in a cargo tank made of quenched and tempered steel as authorized by §173.315(a), Note 14 of this subchapter, or

(ii) The words “NOT FOR Q and T TANKS” when the anhydrous ammonia does not contain 0.2 percent or more water by weight.

(2) *Liquefied petroleum gas.* (i) The word “NONCORROSIVE” or “NONCOR” to indicate the suitability for shipping “Noncorrosive” liquefied petroleum gas in a cargo tank made of quenched and tempered steel as authorized by §173.315(a), Note 15 of this subchapter, or

(ii) The words “NOT FOR Q and T TANKS” for grades of liquefied petroleum gas other than “Noncorrosive”.

(i) *Transportation by water.* Each shipment by water must have the following additional shipping paper entries:

(1) The name of the shipper.

(2) Minimum flash point if 61 °C or below (in °C closed cup (c.c.) in association with the basic description.

(3) For a hazardous material consigned under an “n.o.s.” entry not included in the segregation groups listed in section 3.1.4 of the IMDG Code but belonging, in the opinion of the consignor, to one of these groups, the appropriate segregation group must be shown in association with the basic description (for example, IMDG Code segregation group—1 Acids). When no segregation group is applicable, there is no requirement to indicate that condition.

(j) [Reserved]

(k) *Technical names for “n.o.s.” and other generic descriptions.* Unless otherwise excepted, if a material is described on a shipping paper by one of the proper shipping names identified by the letter “G” in column (1) of the §172.101 Table, the technical name of the hazardous material must be entered in parentheses in association with the basic description. For example “Corrosive liquid, n.o.s., (Octanoyl chloride), 8, UN 1760, II”, or “Corrosive liquid, n.o.s., 8, UN 1760, II (contains Octanoyl chloride)”. The word “contains” may be used in association with the technical name, if appropriate. For

organic peroxides which may qualify for more than one generic listing depending on concentration, the technical name must include the actual concentration being shipped or the concentration range for the appropriate generic listing. For example, “Organic peroxide type B, solid, 5.2, UN 3102 (dibenzoyl peroxide, 52–100%)” or “Organic peroxide type E, solid, 5.2, UN 3108 (dibenzoyl peroxide, paste, <52%)”. Shipping descriptions for toxic materials that meet the criteria of Division 6.1, PG I or II (as specified in §173.132(a) of this subchapter) or Division 2.3 (as specified in §173.115(c) of this subchapter) and are identified by the letter “G” in column (1) of the §172.101 Table, must have the technical name of the toxic constituent entered in parentheses in association with the basic description.

(1) If a hazardous material is a mixture or solution of two or more hazardous materials, the technical names of at least two components most predominately contributing to the hazards of the mixture or solution must be entered on the shipping paper as required by paragraph (k) of this section. For example, “Flammable liquid, corrosive, n.o.s., 3, UN 2924, II (contains Methanol, Potassium hydroxide)”.

(2) The provisions of this paragraph do not apply—

(i) To a material that is a hazardous waste and described using the proper shipping name “Hazardous waste, liquid *or* solid, n.o.s.”, classed as a miscellaneous Class 9, provided the EPA hazardous waste number is included on the shipping paper in association with the basic description, or provided the material is described in accordance with the provisions of §172.203(e) of this part.

(ii) To a material for which the hazard class is to be determined by testing under the criteria in §172.101(c)(11).

(iii) If the n.o.s. description for the material (other than a mixture of hazardous materials of different classes meeting the definitions of more than one hazard class) contains the name of the chemical element or group which is primarily responsible for the material being included in the hazard class indicated.

(iv) If the n.o.s. description for the material (which is a mixture of hazardous materials of different classes meeting the definition of more than one hazard class) contains the name of the chemical element or group responsible for the material meeting the definition of one of these classes. In such cases, only the technical name of the component that is not appropriately identified in the n.o.s. description shall be entered in parentheses.

(1) *Marine pollutants.* (1) If the proper shipping name for a material which is a marine pollutant does not identify by name the component which makes the material a marine pollutant, the name of that component must appear in parentheses in association with the basic description. Where two or more components which make a material a marine pollutant are present, the names of at least two of the components most predominantly contributing to the marine pollutant designation must appear in parentheses in association with the basic description.

(2) The words "Marine Pollutant" shall be entered in association with the basic description for a material which is a marine pollutant.

(3) Except for transportation by vessel, marine pollutants subject to the provisions of 49 CFR 130.11 are excepted from the requirements of paragraph (1) of this section if a phrase indicating the material is an oil is placed in association with the basic description.

(4) Except when transported aboard vessel, marine pollutants in non-bulk packagings are not subject to the requirements of this subchapter (see § 171.4 of this subchapter).

(m) *Poisonous Materials.* Notwithstanding the hazard class to which a material is assigned, for materials that are poisonous by inhalation (see § 171.8 of this subchapter), the words "Poison-Inhalation Hazard" or "Toxic-Inhalation Hazard" and the words "Zone A", "Zone B", "Zone C", or "Zone D" for gases or "Zone A" or "Zone B" for liquids, as appropriate, shall be entered on the shipping paper immediately following the shipping description. The word "Poison" or "Toxic" need not be repeated if it otherwise appears in the shipping description.

(n) *Elevated temperature materials.* If a liquid material in a package meets the definition of an elevated temperature material in § 171.8 of this subchapter, and the fact that it is an elevated temperature material is not disclosed in the proper shipping name (for example, when the words "Molten" or "Elevated temperature" are part of the proper shipping name), the word "HOT" must immediately precede the proper shipping name of the material on the shipping paper.

(o) *Organic peroxides and self-reactive materials.* The description on a shipping paper for a Division 4.1 (self-reactive) material or a Division 5.2 (organic peroxide) material must include the following additional information, as appropriate:

(1) If notification or competent authority approval is required, the shipping paper must contain a statement of approval of the classification and conditions of transport.

(2) For Division 4.1 (self-reactive) and Division 5.2 (organic peroxide) materials that require temperature control during transport, the control and emergency temperature must be included on the shipping paper.

(3) The word "SAMPLE" must be included in association with the basic description when a sample of a Division 4.1 (self-reactive) material (see § 173.224(c)(3) of this subchapter) or Division 5.2 (organic peroxide) material (see § 173.225(b)(2) of this subchapter) is offered for transportation.

[Amdt. 172-29A, 41 FR 40677, Sept. 20, 1976]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 172.203, see the List of CFR Sections Affected which appears in the Finding Aids section of the printed volume and on GPO Access.

§ 172.204 Shipper's certification.

(a) *General.* Except as provided in paragraphs (b) and (c) of this section, each person who offers a hazardous material for transportation shall certify that the material is offered for transportation in accordance with this subchapter by printing (manually or mechanically) on the shipping paper containing the required shipping description the certification contained in paragraph (a)(1) of this section or the certification (declaration) containing

§ 172.204

49 CFR Ch. I (10–1–05 Edition)

the language contained in paragraph (a)(2) of this section.

(1) “This is to certify that the above-named materials are properly classified, described, packaged, marked and labeled, and are in proper condition for transportation according to the applicable regulations of the Department of Transportation.”

NOTE: In line one of the certification the words “herein-named” may be substituted for the words “above-named”.

(2) “I hereby declare that the contents of this consignment are fully and accurately described above by the proper shipping name, and are classified, packaged, marked and labelled/placarded, and are in all respects in proper condition for transport according to applicable international and national governmental regulations.”

(b) *Exceptions.* (1) Except for a hazardous waste, no certification is required for a hazardous material offered for transportation by motor vehicle and transported:

(i) In a cargo tank supplied by the carrier, or

(ii) By the shipper as a private carrier except for a hazardous material that is to be reshipped or transferred from one carrier to another.

(2) No certification is required for the return of an empty tank car which previously contained a hazardous material and which has not been cleaned or purged.

(c) *Transportation by air*—(1) *General.* Certification containing the following language may be used in place of the certification required by paragraph (a) of this section:

I hereby certify that the contents of this consignment are fully and accurately described above by proper shipping name and are classified, packaged, marked and labeled, and in proper condition for carriage by air according to applicable national governmental regulations.

NOTE TO PARAGRAPH (c)(1): In the certification, the word “packed” may be used instead of the word “packaged” until October 1, 2010.

(2) *Certificate in duplicate.* Each person who offers a hazardous material to an aircraft operator for transportation by air shall provide two copies of the certification required in this section. (See § 175.30 of this subchapter.)

(3) *Additional certification requirements.* Effective October 1, 2006, each person who offers a hazardous material for transportation by air must add to the certification required in this section the following statement:

“I declare that all of the applicable air transport requirements have been met.”

(i) Each person who offers any package or overpack of hazardous materials for transport by air must ensure that:

(A) The articles or substances are not prohibited for transport by air (see the § 172.101 Table);

(B) The articles or substances are properly classed, marked and labeled and otherwise in a condition for transport as required by this subchapter;

(C) The articles or substances are packaged in accordance with all the applicable air transport requirements, including appropriate types of packaging that conform to the packing requirements and the “A” Special Provisions in § 172.102; inner packaging and maximum quantity per package limits; the compatibility requirements (see, for example, § 173.24 of this subchapter); and requirements for closure for both inner and outer packagings, absorbent materials, and pressure differential in § 173.27 of this subchapter. Other requirements may also apply. For example, single packagings may be prohibited, inner packaging may need to be packed in intermediate packagings, and certain materials may be required to be transported in packagings meeting a more stringent performance level.

(ii) [Reserved]

(4) *Radioactive material.* Each person who offers any radioactive material for transportation aboard a passenger-carrying aircraft shall sign (mechanically or manually) a printed certificate stating that the shipment contains radioactive material intended for use in, or incident to, research, or medical diagnosis or treatment.

(d) *Signature.* The certifications required by paragraph (a) or (c) of this section:

(1) Must be legibly signed by a principal, officer, partner, or employee of the shipper or his agent; and

(2) May be legibly signed manually, by typewriter, or by other mechanical means.

[Amdt. 172-29A, 41 FR 40677, Sept. 20, 1976]

EDITORIAL NOTE: For FEDERAL REGISTER citations affecting § 172.204, see the List of CFR Sections Affected which appears in the Finding Aids section of the printed volume and on GPO Access.

§ 172.205 Hazardous waste manifest.

(a) No person may offer, transport, transfer, or deliver a hazardous waste (waste) unless an EPA Form 8700-22 and 8700-22A (when necessary) hazardous waste manifest (manifest) is prepared in accordance with 40 CFR 262.20 and is signed, carried, and given as required of that person by this section.

(b) The shipper (generator) shall prepare the manifest in accordance with 40 CFR part 262.

(c) The original copy of the manifest must be dated by, and bear the handwritten signature of, the person representing:

(1) The shipper (generator) of the waste at the time it is offered for transportation, and

(2) The initial carrier accepting the waste for transportation.

(d) A copy of the manifest must be dated by, and bear the handwritten signature of the person representing:

(1) Each subsequent carrier accepting the waste for transportation, at the time of acceptance, and

(2) The designated facility receiving the waste, upon receipt.

(e) A copy of the manifest bearing all required dates and signatures must be:

(1) Given to a person representing each carrier accepting the waste for transportation,

(2) Carried during transportation in the same manner as required by this subchapter for shipping papers,

(3) Given to a person representing the designated facility receiving the waste,

(4) Returned to the shipper (generator) by the carrier that transported the waste from the United States to a foreign destination with a notation of the date of departure from the United States, and

(5) Retained by the shipper (generator) and by the initial and each subsequent carrier for three years from the

date the waste was accepted by the initial carrier. Each retained copy must bear all required signatures and dates up to and including those entered by the next person who received the waste.

(f) *Transportation by rail.* Notwithstanding the requirements of paragraphs (d) and (e) of this section, the following requirements apply:

(1) When accepting hazardous waste from a non-rail transporter, the initial rail transporter must:

(i) Sign and date the manifest acknowledging acceptance of the hazardous waste;

(ii) Return a signed copy of the manifest to the non-rail transporter;

(iii) Forward at least three copies of the manifest to:

(A) The next non-rail transporter, if any;

(B) The designated facility, if the shipment is delivered to that facility by rail; or

(C) The last rail transporter designated to handle the waste in the United States; and

(iv) Retain one copy of the manifest and rail shipping paper in accordance with 40 CFR 263.22.

(2) Rail transporters must ensure that a shipping paper containing all the information required on the manifest (excluding the EPA identification numbers, generator certification and signatures) and, for exports, an EPA Acknowledgment of Consent accompanies the hazardous waste at all times. Intermediate rail transporters are not required to sign either the manifest or shipping paper.

(3) When delivering hazardous waste to the designated facility, a rail transporter must:

(i) Obtain the date of delivery and handwritten signature of the owner or operator of the designated facility on the manifest or the shipping paper (if the manifest has not been received by the facility); and

(ii) Retain a copy of the manifest or signed shipping paper in accordance with 40 CFR 263.22.

(4) When delivering hazardous waste to a non-rail transporter, a rail transporter must:

(i) Obtain the date of delivery and the handwritten signature of the next

§ 172.300

49 CFR Ch. I (10–1–05 Edition)

non-rail transporter on the manifest; and

(ii) Retain a copy of the manifest in accordance with 40 CFR 263.22.

(5) Before accepting hazardous waste from a rail transporter, a non-rail transporter must sign and date the manifest and provide a copy to the rail transporter.

(g) The person delivering a hazardous waste to an initial rail carrier shall send a copy of the manifest, dated and signed by a representative of the rail carrier, to the person representing the designated facility.

(h) A hazardous waste manifest required by 40 CFR part 262, containing all of the information required by this subpart, may be used as the shipping paper required by this subpart.

(i) The shipping description for a hazardous waste must be modified as required by § 172.101(c)(9).

[Amdt. 172–58, 45 FR 34698, May 22, 1980, as amended by Amdt. 172–90, 49 FR 10510, Mar. 20, 1984; 49 FR 11184, Mar. 26, 1984; Amdt. 172–248, 61 FR 28675, June 5, 1996; 70 FR 34075, June 13, 2005]

Subpart D—Marking

§ 172.300 Applicability.

(a) Each person who offers a hazardous material for transportation shall mark each package, freight container, and transport vehicle containing the hazardous material in the manner required by this subpart.

(b) When assigned the function by this subpart, each carrier that transports a hazardous material shall mark each package, freight container, and transport vehicle containing the hazardous material in the manner required by this subpart.

[Amdt. 172–101, 45 FR 74666, Nov. 10, 1980]

§ 172.301 General marking requirements for non-bulk packagings.

(a) *Proper shipping name and identification number.* (1) Except as otherwise provided by this subchapter, each person who offers a hazardous material for transportation in a non-bulk packaging must mark the package with the proper shipping name and identification number (preceded by “UN” or “NA,” as appropriate) for the material as shown

in the § 172.101 Table. Identification numbers are not required on packagings that contain only ORM-D materials or limited quantities, as defined in § 171.8 of this subchapter, except for limited quantities marked in accordance with the marking requirements in § 172.315.

(2) The proper shipping name for a hazardous waste (as defined in § 171.8 of this subchapter) is not required to include the word “waste” if the package bears the EPA marking prescribed by 40 CFR 262.32.

(3) *Large quantities of a single hazardous material in non-bulk packages.* A transport vehicle or freight container containing only a single hazardous material in non-bulk packages must be marked, on each side and each end as specified in the § 172.332 or § 172.336, with the identification number specified for the hazardous material in the § 172.101 Table, subject to the following provisions and limitations:

(i) Each package is marked with the same proper shipping name and identification number;

(ii) The aggregate gross weight of the hazardous material is 4,000 kg (8,820 pounds) or more;

(iii) All of the hazardous material is loaded at one loading facility;

(iv) The transport vehicle or freight container contains no other material, hazardous or otherwise; and

(v) The identification number marking requirement of this paragraph (a)(3) does not apply to Class 1, Class 7, or to non-bulk packagings for which identification numbers are not required.

(b) *Technical names.* In addition to the marking required by paragraph (a) of this section, each non-bulk packaging containing hazardous materials subject to the provisions of § 172.203(k) of this part shall be marked with the technical name in parentheses in association with the proper shipping name in accordance with the requirements and exceptions specified for display of technical descriptions on shipping papers in § 172.203(k) of this part.

(c) *Exemption packagings.* The outside of each package authorized by an exemption shall be plainly and durably marked “DOT-E” followed by the exemption number assigned.

§ 172.600

(b) In addition to conformance with § 172.519, the background on the CLASS 9 placard must be white with seven black vertical stripes on the top half extending from the top of the placard to one inch above the horizontal centerline. The black vertical stripes must be spaced so that, visually, they appear equal in width to the six white spaces between them. The space below the vertical lines must be white with the class number 9 underlined and centered at the bottom.

[Amdt. 172-123, 56 FR 66264, Dec. 20, 1991, as amended at 57 FR 45460, Oct. 1, 1992]

Subpart G—Emergency Response Information

§ 172.600 Applicability and general requirements.

(a) *Scope.* Except as provided in paragraph (d) of this section, this subpart prescribes requirements for providing and maintaining emergency response information during transportation and at facilities where hazardous materials are loaded for transportation, stored incidental to transportation or otherwise handled during any phase of transportation.

(b) *Applicability.* This subpart applies to persons who offer for transportation, accept for transportation, transfer or otherwise handle hazardous materials during transportation.

(c) *General requirements.* No person to whom this subpart applies may offer for transportation, accept for transportation, transfer, store or otherwise handle during transportation a hazardous material unless:

(1) Emergency response information conforming to this subpart is immediately available for use at all times the hazardous material is present; and

(2) Emergency response information, including the emergency response telephone number, required by this subpart is immediately available to any person who, as a representative of a Federal, State or local government agency, responds to an incident involving a hazardous material, or is conducting an investigation which involves a hazardous material.

(d) *Exceptions.* The requirements of this subpart do not apply to hazardous material which is excepted from the

49 CFR Ch. I (10-1-04 Edition)

shipping paper requirements of this subchapter or a material properly classified as an ORM-D.

[Amdt. 172-116, 54 FR 27145, June 27, 1989; 54 FR 28750, July 5, 1989, as amended at 55 FR 33712, Aug. 17, 1990; 172-127, 59 FR 49133, Sept. 26, 1994; Amdt. 172-149, 61 FR 27173, May 30, 1996]

§ 172.602 Emergency response information.

(a) *Information required.* For purposes of this subpart, the term “emergency response information” means information that can be used in the mitigation of an incident involving hazardous materials and, as a minimum, must contain the following information:

(1) The basic description and technical name of the hazardous material as required by §§ 172.202 and 172.203(k), the ICAO Technical Instructions, the IMDG Code, or the TDG Regulations, as appropriate (IBR, see § 171.7 of this subchapter);

(2) Immediate hazards to health;

(3) Risks of fire or explosion;

(4) Immediate precautions to be taken in the event of an accident or incident;

(5) Immediate methods for handling fires;

(6) Initial methods for handling spills or leaks in the absence of fire; and

(7) Preliminary first aid measures.

(b) *Form of information.* The information required for a hazardous material by paragraph (a) of this section must be:

(1) Printed legibly in English;

(2) Available for use away from the package containing the hazardous material; and

(3) Presented—

(i) On a shipping paper;

(ii) In a document, other than a shipping paper, that includes both the basic description and technical name of the hazardous material as required by §§ 172.202 and 172.203(k), the ICAO Technical Instructions, the IMDG Code, or the TDG Regulations, as appropriate, and the emergency response information required by this subpart (e.g., a material safety data sheet); or

(iii) Related to the information on a shipping paper, a written notification to pilot-in-command, or a dangerous cargo manifest, in a separate document

(e.g., an emergency response guidance document), in a manner that cross-references the description of the hazardous material on the shipping paper with the emergency response information contained in the document. Aboard aircraft, the ICAO “Emergency Response Guidance for Aircraft Incidents Involving Dangerous Goods” and, aboard vessels, the IMO “Emergency Procedures for Ships Carrying Dangerous Goods”, or equivalent documents, may be used to satisfy the requirements of this section for a separate document.

(c) *Maintenance of information.* Emergency response information shall be maintained as follows:

(1) *Carriers.* Each carrier who transports a hazardous material shall maintain the information specified in paragraph (a) of this section and § 172.606 of this part in the same manner as prescribed for shipping papers, except that the information must be maintained in the same manner aboard aircraft as the notification of pilot-in-command, and aboard vessels in the same manner as the dangerous cargo manifest. This information must be immediately accessible to train crew personnel, drivers of motor vehicles, flight crew members, and bridge personnel on vessels for use in the event of incidents involving hazardous materials.

(2) *Facility operators.* Each operator of a facility where a hazardous material is received, stored or handled during transportation, shall maintain the information required by paragraph (a) of this section whenever the hazardous material is present. This information must be in a location that is immediately accessible to facility personnel in the event of an incident involving the hazardous material.

[Amdt. 172-116, 54 FR 27146, June 27, 1989; 54 FR 28750, July 5, 1989, as amended by Amdt. 172-116, 55 FR 875, Jan. 10, 1990; Amdt. 172-151, 62 FR 1234, Jan. 8, 1997; 66 FR 45379, Aug. 28, 2001; 68 FR 75741, Dec. 31, 2003]

§ 172.604 Emergency response telephone number.

(a) A person who offers a hazardous material for transportation must provide an emergency response telephone number, including the area code or international access code, for use in

the event of an emergency involving the hazardous material. The telephone number must be—

(1) Monitored at all times the hazardous material is in transportation, including storage incidental to transportation;

(2) The number of a person who is either knowledgeable of the hazardous material being shipped and has comprehensive emergency response and incident mitigation information for that material, or has immediate access to a person who possesses such knowledge and information; and

(3) Entered on a shipping paper, as follows:

(i) Immediately following the description of the hazardous material required by subpart C of this part; or

(ii) Entered once on the shipping paper in a clearly visible location. This provision may be used only if the telephone number applies to each hazardous material entered on the shipping paper, and if it is indicated that the telephone number is for emergency response information (for example: “EMERGENCY CONTACT: * * *”).

(b) The telephone number required by paragraph (a) of this section must be the number of the person offering the hazardous material for transportation or the number of an agency or organization capable of, and accepting responsibility for, providing the detailed information concerning the hazardous material. A person offering a hazardous material for transportation who lists the telephone number of an agency or organization shall ensure that agency or organization has received current information on the material, as required by paragraph (a)(2) of this section before it is offered for transportation.

(c) The requirements of this section do not apply to—

(1) Hazardous materials that are offered for transportation under the provisions applicable to limited quantities; and

(2) Materials properly described under the following shipping names:

Battery powered equipment
 Battery powered vehicle
 Carbon dioxide, solid
 Castor bean
 Castor flake

(e.g., an emergency response guidance document), in a manner that cross-references the description of the hazardous material on the shipping paper with the emergency response information contained in the document. Aboard aircraft, the ICAO "Emergency Response Guidance for Aircraft Incidents Involving Dangerous Goods" and, aboard vessels, the IMO "Emergency Procedures for Ships Carrying Dangerous Goods", or equivalent documents, may be used to satisfy the requirements of this section for a separate document.

(c) *Maintenance of information.* Emergency response information shall be maintained as follows:

(1) *Carriers.* Each carrier who transports a hazardous material shall maintain the information specified in paragraph (a) of this section and § 172.606 of this part in the same manner as prescribed for shipping papers, except that the information must be maintained in the same manner aboard aircraft as the notification of pilot-in-command, and aboard vessels in the same manner as the dangerous cargo manifest. This information must be immediately accessible to train crew personnel, drivers of motor vehicles, flight crew members, and bridge personnel on vessels for use in the event of incidents involving hazardous materials.

(2) *Facility operators.* Each operator of a facility where a hazardous material is received, stored or handled during transportation, shall maintain the information required by paragraph (a) of this section whenever the hazardous material is present. This information must be in a location that is immediately accessible to facility personnel in the event of an incident involving the hazardous material.

[Amdt. 172-116, 54 FR 27146, June 27, 1989; 54 FR 28750, July 5, 1989, as amended by Amdt. 172-116, 55 FR 875, Jan. 10, 1990; Amdt. 172-151, 62 FR 1234, Jan. 8, 1997; 66 FR 45379, Aug. 28, 2001; 68 FR 75741, Dec. 31, 2003]

§ 172.604 Emergency response telephone number.

(a) A person who offers a hazardous material for transportation must provide an emergency response telephone number, including the area code or international access code, for use in

the event of an emergency involving the hazardous material. The telephone number must be—

(1) Monitored at all times the hazardous material is in transportation, including storage incidental to transportation;

(2) The number of a person who is either knowledgeable of the hazardous material being shipped and has comprehensive emergency response and incident mitigation information for that material, or has immediate access to a person who possesses such knowledge and information; and

(3) Entered on a shipping paper, as follows:

(i) Immediately following the description of the hazardous material required by subpart C of this part; or

(ii) Entered once on the shipping paper in a clearly visible location. This provision may be used only if the telephone number applies to each hazardous material entered on the shipping paper, and if it is indicated that the telephone number is for emergency response information (for example: "EMERGENCY CONTACT: * * *").

(b) The telephone number required by paragraph (a) of this section must be the number of the person offering the hazardous material for transportation or the number of an agency or organization capable of, and accepting responsibility for, providing the detailed information concerning the hazardous material. A person offering a hazardous material for transportation who lists the telephone number of an agency or organization shall ensure that agency or organization has received current information on the material, as required by paragraph (a)(2) of this section before it is offered for transportation.

(c) The requirements of this section do not apply to—

(1) Hazardous materials that are offered for transportation under the provisions applicable to limited quantities; and

(2) Materials properly described under the following shipping names:

Battery powered equipment
 Battery powered vehicle
 Carbon dioxide, solid
 Castor bean
 Castor flake

§ 172.606

Castor meal
Castor pomace
Consumer commodity
Dry ice
Engines, internal combustion
Fish meal, stabilized
Fish scrap, stabilized
Refrigerating machine
Vehicle, flammable gas powered
Vehicle, flammable liquid powered
Wheelchair, electric

[Amdt. 172-116, 54 FR 27145, June 27, 1989, as amended at 55 FR 33713, Aug. 17, 1990; Amdt. 172-127, 59 FR 49133, Sept. 26, 1994; Amdt. 172-149, 61 FR 27173, May 30, 1996; 65 FR 50460, Aug. 18, 2000; 65 FR 58628, Sept. 29, 2000; 66 FR 45182, Aug. 28, 2001]

§ 172.606 Carrier information contact.

(a) Each carrier who transports or accepts for transportation a hazardous material for which a shipping paper is required shall instruct the operator of a motor vehicle, train, aircraft, or vessel to contact the carrier (e.g., by telephone or mobile radio) in the event of an incident involving the hazardous material.

(b) For transportation by highway, if a transport vehicle, (e.g., a semi-trailer or freight container-on-chassis) contains hazardous material for which a shipping paper is required and the vehicle is separated from its motive power and parked at a location other than a facility operated by the consignor or consignee or a facility (e.g., a carrier's terminal or a marine terminal) subject to the provisions of §172.602(c)(2), the carrier shall—

(1) Mark the transport vehicle with the telephone number of the motor carrier on the front exterior near the brake hose and electrical connections or on a label, tag, or sign attached to the vehicle at the brake hose or electrical connection; or

(2) Have the shipping paper and emergency response information readily available on the transport vehicle.

(c) The requirements specified in paragraph (b) of this section do not apply to an unattended motor vehicle separated from its motive power when the motor vehicle is marked on an orange panel, a placard, or a plain white square-on-point configuration with the identification number of each hazardous material loaded therein, and the

49 CFR Ch. I (10-1-04 Edition)

marking or placard is visible on the outside of the motor vehicle.

[Amdt. 172-151, 62 FR 1234, Jan. 8, 1997, as amended at 62 FR 39398 and 39409, July 22, 1997; 63 FR 16076, Apr. 1, 1998]

Subpart H—Training

SOURCE: Amdt. 172-126, 57 FR 20952, May 15, 1992, unless otherwise noted.

§ 172.700 Purpose and scope.

(a) *Purpose.* This subpart prescribes requirements for training hazmat employees.

(b) *Scope.* Training as used in this subpart means a systematic program that ensures a hazmat employee has familiarity with the general provisions of this subchapter, is able to recognize and identify hazardous materials, has knowledge of specific requirements of this subchapter applicable to functions performed by the employee, and has knowledge of emergency response information, self-protection measures and accident prevention methods and procedures (see §172.704).

(c) *Modal-specific training requirements.* Additional training requirements for the individual modes of transportation are prescribed in parts 174, 175, 176, and 177 of this subchapter.

§ 172.701 Federal-State relationship.

This subpart and the parts referenced in §172.700(c) prescribe minimum training requirements for the transportation of hazardous materials. For motor vehicle drivers, however, a State may impose more stringent training requirements only if those requirements—

(a) Do not conflict with the training requirements in this subpart and in part 177 of this subchapter; and

(b) Apply only to drivers domiciled in that State.

§ 172.702 Applicability and responsibility for training and testing.

(a) A hazmat employer shall ensure that each of its hazmat employees is trained in accordance with the requirements prescribed in this subpart.

(b) Except as provided in §172.704(c)(1), a hazmat employee who performs any function subject to the

Battery powered equipment
 Battery powered vehicle
 Carbon dioxide, solid
 Castor bean
 Castor flake
 Castor meal
 Castor pomace
 Consumer commodity
 Dry ice
 Engines, internal combustion
 Fish meal, stabilized
 Fish scrap, stabilized
 Refrigerating machine
 Vehicle, flammable gas powered
 Vehicle, flammable liquid powered
 Wheelchair, electric

[Amdt. 172-116, 54 FR 27145, June 27, 1989, as amended at 55 FR 33713, Aug. 17, 1990; Amdt. 172-127, 59 FR 49133, Sept. 26, 1994; Amdt. 172-149, 61 FR 27173, May 30, 1996; 65 FR 50460, Aug. 18, 2000; 65 FR 58628, Sept. 29, 2000; 66 FR 45182, Aug. 28, 2001; 69 FR 64473, Nov. 4, 2004]

§ 172.606 Carrier information contact.

(a) Each carrier who transports or accepts for transportation a hazardous material for which a shipping paper is required shall instruct the operator of a motor vehicle, train, aircraft, or vessel to contact the carrier (e.g., by telephone or mobile radio) in the event of an incident involving the hazardous material.

(b) For transportation by highway, if a transport vehicle, (e.g., a semi-trailer or freight container-on-chassis) contains hazardous material for which a shipping paper is required and the vehicle is separated from its motive power and parked at a location other than a facility operated by the consignor or consignee or a facility (e.g., a carrier's terminal or a marine terminal) subject to the provisions of §172.602(c)(2), the carrier shall—

(1) Mark the transport vehicle with the telephone number of the motor carrier on the front exterior near the brake hose and electrical connections or on a label, tag, or sign attached to the vehicle at the brake hose or electrical connection; or

(2) Have the shipping paper and emergency response information readily available on the transport vehicle.

(c) The requirements specified in paragraph (b) of this section do not apply to an unattended motor vehicle separated from its motive power when the motor vehicle is marked on an orange panel, a placard, or a plain white

square-on-point configuration with the identification number of each hazardous material loaded therein, and the marking or placard is visible on the outside of the motor vehicle.

[Amdt. 172-151, 62 FR 1234, Jan. 8, 1997, as amended at 62 FR 39398 and 39409, July 22, 1997; 63 FR 16076, Apr. 1, 1998]

Subpart H—Training

SOURCE: Amdt. 172-126, 57 FR 20952, May 15, 1992, unless otherwise noted.

§ 172.700 Purpose and scope.

(a) *Purpose.* This subpart prescribes requirements for training hazmat employees.

(b) *Scope.* Training as used in this subpart means a systematic program that ensures a hazmat employee has familiarity with the general provisions of this subchapter, is able to recognize and identify hazardous materials, has knowledge of specific requirements of this subchapter applicable to functions performed by the employee, and has knowledge of emergency response information, self-protection measures and accident prevention methods and procedures (see §172.704).

(c) *Modal-specific training requirements.* Additional training requirements for the individual modes of transportation are prescribed in parts 174, 175, 176, and 177 of this subchapter.

§ 172.701 Federal-State relationship.

This subpart and the parts referenced in §172.700(c) prescribe minimum training requirements for the transportation of hazardous materials. For motor vehicle drivers, however, a State may impose more stringent training requirements only if those requirements—

(a) Do not conflict with the training requirements in this subpart and in part 177 of this subchapter; and

(b) Apply only to drivers domiciled in that State.

§ 172.702 Applicability and responsibility for training and testing.

(a) A hazmat employer shall ensure that each of its hazmat employees is trained in accordance with the requirements prescribed in this subpart.

§ 172.704

49 CFR Ch. I (10–1–05 Edition)

(b) Except as provided in § 172.704(c)(1), a hazmat employee who performs any function subject to the requirements of this subchapter may not perform that function unless instructed in the requirements of this subchapter that apply to that function. It is the duty of each hazmat employer to comply with the applicable requirements of this subchapter and to thoroughly instruct each hazmat employee in relation thereto.

(c) Training may be provided by the hazmat employer or other public or private sources.

(d) A hazmat employer shall ensure that each of its hazmat employees is tested by appropriate means on the training subjects covered in § 172.704.

[Amdt. 172–126, 57 FR 20952, May 15, 1992; 57 FR 22182, May 27, 1992, as amended by Amdt. 172–149, 61 FR 27173, May 30, 1996]

§ 172.704 Training requirements.

(a) Hazmat employee training must include the following:

(1) *General awareness/familiarization training.* Each hazmat employee shall be provided general awareness/familiarization training designed to provide familiarity with the requirements of this subchapter, and to enable the employee to recognize and identify hazardous materials consistent with the hazard communication standards of this subchapter.

(2) *Function-specific training.* (i) Each hazmat employee shall be provided function-specific training concerning requirements of this subchapter, or exemptions issued under subchapter A of this chapter, which are specifically applicable to the functions the employee performs.

(ii) As an alternative to function-specific training on the requirements of this subchapter, training relating to the requirements of the ICAO Technical Instructions and the IMDG Code may be provided to the extent such training addresses functions authorized by §§ 171.11 and 171.12 of this subchapter.

(3) *Safety training.* Each hazmat employee shall receive safety training concerning—

(i) Emergency response information required by subpart G of part 172;

(ii) Measures to protect the employee from the hazards associated with hazardous materials to which they may be exposed in the work place, including specific measures the hazmat employer has implemented to protect employees from exposure; and

(iii) Methods and procedures for avoiding accidents, such as the proper procedures for handling packages containing hazardous materials.

(4) *Security awareness training.* No later than the date of the first scheduled recurrent training after March 25, 2003, and in no case later than March 24, 2006, each hazmat employee must receive training that provides an awareness of security risks associated with hazardous materials transportation and methods designed to enhance transportation security. This training must also include a component covering how to recognize and respond to possible security threats. After March 25, 2003, new hazmat employees must receive the security awareness training required by this paragraph within 90 days after employment.

(5) *In-depth security training.* By December 22, 2003, each hazmat employee of a person required to have a security plan in accordance with subpart I of this part must be trained concerning the security plan and its implementation. Security training must include company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure.

(b) *OSHA, EPA, and other training.* Training conducted by employers to comply with the hazard communication programs required by the Occupational Safety and Health Administration of the Department of Labor (29 CFR 1910.120 or 1910.1200) or the Environmental Protection Agency (40 CFR 311.1), or training conducted by employers to comply with security training programs required by other Federal or international agencies, may be used to satisfy the training requirements in paragraph (a) of this section to the extent that such training addresses the training components specified in paragraph (a) of this section.

§ 172.704

49 CFR Ch. I (10–1–05 Edition)

(b) Except as provided in § 172.704(c)(1), a hazmat employee who performs any function subject to the requirements of this subchapter may not perform that function unless instructed in the requirements of this subchapter that apply to that function. It is the duty of each hazmat employer to comply with the applicable requirements of this subchapter and to thoroughly instruct each hazmat employee in relation thereto.

(c) Training may be provided by the hazmat employer or other public or private sources.

(d) A hazmat employer shall ensure that each of its hazmat employees is tested by appropriate means on the training subjects covered in § 172.704.

[Amdt. 172–126, 57 FR 20952, May 15, 1992; 57 FR 22182, May 27, 1992, as amended by Amdt. 172–149, 61 FR 27173, May 30, 1996]

§ 172.704 Training requirements.

(a) Hazmat employee training must include the following:

(1) *General awareness/familiarization training.* Each hazmat employee shall be provided general awareness/familiarization training designed to provide familiarity with the requirements of this subchapter, and to enable the employee to recognize and identify hazardous materials consistent with the hazard communication standards of this subchapter.

(2) *Function-specific training.* (i) Each hazmat employee shall be provided function-specific training concerning requirements of this subchapter, or exemptions issued under subchapter A of this chapter, which are specifically applicable to the functions the employee performs.

(ii) As an alternative to function-specific training on the requirements of this subchapter, training relating to the requirements of the ICAO Technical Instructions and the IMDG Code may be provided to the extent such training addresses functions authorized by §§ 171.11 and 171.12 of this subchapter.

(3) *Safety training.* Each hazmat employee shall receive safety training concerning—

(i) Emergency response information required by subpart G of part 172;

(ii) Measures to protect the employee from the hazards associated with hazardous materials to which they may be exposed in the work place, including specific measures the hazmat employer has implemented to protect employees from exposure; and

(iii) Methods and procedures for avoiding accidents, such as the proper procedures for handling packages containing hazardous materials.

(4) *Security awareness training.* No later than the date of the first scheduled recurrent training after March 25, 2003, and in no case later than March 24, 2006, each hazmat employee must receive training that provides an awareness of security risks associated with hazardous materials transportation and methods designed to enhance transportation security. This training must also include a component covering how to recognize and respond to possible security threats. After March 25, 2003, new hazmat employees must receive the security awareness training required by this paragraph within 90 days after employment.

(5) *In-depth security training.* By December 22, 2003, each hazmat employee of a person required to have a security plan in accordance with subpart I of this part must be trained concerning the security plan and its implementation. Security training must include company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure.

(b) *OSHA, EPA, and other training.* Training conducted by employers to comply with the hazard communication programs required by the Occupational Safety and Health Administration of the Department of Labor (29 CFR 1910.120 or 1910.1200) or the Environmental Protection Agency (40 CFR 311.1), or training conducted by employers to comply with security training programs required by other Federal or international agencies, may be used to satisfy the training requirements in paragraph (a) of this section to the extent that such training addresses the training components specified in paragraph (a) of this section.

(c) *Initial and recurrent training*—(1) *Initial training.* A new hazmat employee, or a hazmat employee who changes job functions may perform those functions prior to the completion of training provided—

(i) The employee performs those functions under the direct supervision of a properly trained and knowledgeable hazmat employee; and

(ii) The training is completed within 90 days after employment or a change in job function.

(2) *Recurrent training.* A hazmat employee shall receive the training required by this subpart at least once every three years.

(3) *Relevant Training.* Relevant training received from a previous employer or other source may be used to satisfy the requirements of this subpart provided a current record of training is obtained from hazmat employees' previous employer.

(4) *Compliance.* Each hazmat employer is responsible for compliance with the requirements of this subchapter regardless of whether the training required by this subpart has been completed.

(d) *Recordkeeping.* A record of current training, inclusive of the preceding three years, in accordance with this section shall be created and retained by each hazmat employer for as long as that employee is employed by that employer as a hazmat employee and for 90 days thereafter. The record shall include:

(1) The hazmat employee's name;

(2) The most recent training completion date of the hazmat employee's training;

(3) A description, copy, or the location of the training materials used to meet the requirements in paragraph (a) of this section;

(4) The name and address of the person providing the training; and

(5) Certification that the hazmat employee has been trained and tested, as required by this subpart.

(e) *Limitation.* A hazmat employee who repairs, modifies, reconditions, or tests packagings as qualified for use in the transportation of hazardous materials, and who does not perform any other function subject to the requirements of this subchapter, is not subject

to the safety training requirement of paragraph (a)(3) of this section.

[Amdt. 172-126, 57 FR 20952, May 15, 1992, as amended by Amdt. 172-126, 58 FR 5851, Jan. 22, 1993; Amdt. 172-145, 60 FR 49110, Sept. 21, 1995; Amdt. 172-149, 61 FR 27173, May 30, 1996; 65 FR 50460, Aug. 18, 2000; 68 FR 14521, Mar. 25, 2003]

Subpart I—Security Plans

SOURCE: 68 FR 14521, Mar. 25, 2003, unless otherwise noted.

§ 172.800 Purpose and applicability.

(a) *Purpose.* This subpart prescribes requirements for development and implementation of plans to address security risks related to the transportation of hazardous materials in commerce.

(b) *Applicability.* By September 25, 2003, each person who offers for transportation in commerce or transports in commerce one or more of the following hazardous materials must develop and adhere to a security plan for hazardous materials that conforms to the requirements of this subpart:

(1) A highway route-controlled quantity of a Class 7 (radioactive) material, as defined in §173.403 of this subchapter, in a motor vehicle, rail car, or freight container;

(2) More than 25 kg (55 pounds) of a Division 1.1, 1.2, or 1.3 (explosive) material in a motor vehicle, rail car, or freight container;

(3) More than one L (1.06 qt) per package of a material poisonous by inhalation, as defined in §171.8 of this subchapter, that meets the criteria for Hazard Zone A, as specified in §§173.116(a) or 173.133(a) of this subchapter;

(4) A shipment of a quantity of hazardous materials in a bulk packaging having a capacity equal to or greater than 13,248 L (3,500 gallons) for liquids or gases or more than 13.24 cubic meters (468 cubic feet) for solids;

(5) A shipment in other than a bulk packaging of 2,268 kg (5,000 pounds) gross weight or more of one class of hazardous materials for which placarding of a vehicle, rail car, or freight container is required for that class under the provisions of subpart F of this part;

- 177.804 Compliance with Federal Motor Carrier Safety Regulations.
 177.810 Vehicular tunnels.
 177.816 Driver training.
 177.817 Shipping papers.
 177.823 Movement of motor vehicles in emergency situations.

Subpart B—Loading and Unloading

- 177.834 General requirements.
 177.835 Class 1 materials.
 177.837 Class 3 materials.
 177.838 Class 4 (flammable solid) materials, Class 5 (oxidizing) materials, and Division 4.2 (pyroforic liquid) materials.
 177.839 Class 8 (corrosive) materials.
 177.840 Class 2 (gases) materials.
 177.841 Division 6.1 and Division 2.3 materials.
 177.842 Class 7 (radioactive) material.
 177.843 Contamination of vehicles.

Subpart C—Segregation and Separation Chart of Hazardous Materials

- 177.848 Segregation of hazardous materials.

Subpart D—Vehicles and Shipments in Transit; Accidents

- 177.854 Disabled vehicles and broken or leaking packages; repairs.

Subpart E—Regulations Applying to Hazardous Material on Motor Vehicles Carrying Passengers for Hire

- 177.870 Regulations for passenger carrying vehicles.

AUTHORITY: 49 U.S.C. 5101–5127; 49 CFR 1.53.

Subpart A—General Information and Regulations

§ 177.800 Purpose and scope of this part and responsibility for compliance and training.

(a) *Purpose and scope.* This part prescribes requirements, in addition to those contained in parts 171, 172, 173, 178 and 180 of this subchapter, that are applicable to the acceptance and transportation of hazardous materials by private, common, or contract carriers by motor vehicle.

(b) *Responsibility for compliance.* Unless this subchapter specifically provides that another person shall perform a particular duty, each carrier, including a connecting carrier, shall perform the duties specified and comply with all applicable requirements in this part

and shall ensure its hazmat employees receive training in relation thereto.

(c) *Responsibility for training.* A carrier may not transport a hazardous material by motor vehicle unless each of its hazmat employees involved in that transportation is trained as required by this part and subpart H of part 172 of this subchapter.

(d) *No unnecessary delay in movement of shipments.* All shipments of hazardous materials must be transported without unnecessary delay, from and including the time of commencement of the loading of the hazardous material until its final unloading at destination.

[Amdt. 177–79, 57 FR 20954, May 15, 1992, as amended by Amdt.177–86, 61 FR 18933, Apr. 29, 1996]

§ 177.801 Unacceptable hazardous materials shipments.

No person may accept for transportation or transport by motor vehicle a forbidden material or hazardous material that is not prepared in accordance with the requirements of this subchapter.

[Amdt. 177–87, 61 FR 27175, May 30, 1996]

§ 177.802 Inspection.

Records, equipment, packagings and containers under the control of a motor carrier, insofar as they affect safety in transportation of hazardous materials by motor vehicle, must be made available for examination and inspection by a duly authorized representative of the Department.

[Amdt. 177–71, 54 FR 25015, June 12, 1989]

§ 177.804 Compliance with Federal Motor Carrier Safety Regulations.

Motor carriers and other persons subject to this part must comply with 49 CFR part 383 and 49 CFR parts 390 through 397 (excluding §§ 397.3 and 397.9) to the extent those regulations apply.

[68 FR 23842, May 5, 2003]

§ 177.810 Vehicular tunnels.

Except as regards Class 7 (radioactive) materials, nothing contained in parts 170–189 of this subchapter shall be so construed as to nullify or supersede regulations established and published

§ 177.816

under authority of State statute or municipal ordinance regarding the kind, character, or quantity of any hazardous material permitted by such regulations to be transported through any urban vehicular tunnel used for mass transportation.

[Amdt. 177-52, 46 FR 5316, Jan. 19, 1981, as amended by Amdt. 177-78, 55 FR 52710, Dec. 21, 1990; 62 FR 51561, Oct. 1, 1997]

§ 177.816 Driver training.

(a) In addition to the training requirements of §177.800, no carrier may transport, or cause to be transported, a hazardous material unless each hazmat employee who will operate a motor vehicle has been trained in the applicable requirements of 49 CFR parts 390 through 397 and the procedures necessary for the safe operation of that motor vehicle. Driver training shall include the following subjects:

- (1) Pre-trip safety inspection;
 - (2) Use of vehicle controls and equipment, including operation of emergency equipment;
 - (3) Operation of vehicle, including turning, backing, braking, parking, handling, and vehicle characteristics including those that affect vehicle stability, such as effects of braking and curves, effects of speed on vehicle control, dangers associated with maneuvering through curves, dangers associated with weather or road conditions that a driver may experience (e.g., blizzards, mountainous terrain, high winds), and high center of gravity;
 - (4) Procedures for maneuvering tunnels, bridges, and railroad crossings;
 - (5) Requirements pertaining to attendance of vehicles, parking, smoking, routing, and incident reporting; and
 - (6) Loading and unloading of materials, including—
 - (i) Compatibility and segregation of cargo in a mixed load;
 - (ii) Package handling methods; and
 - (iii) Load securement.
- (b) *Specialized requirements for cargo tanks and portable tanks.* In addition to the training requirement of paragraph (a) of this section, each person who operates a cargo tank or a vehicle with a portable tank with a capacity of 1,000 gallons or more must receive training applicable to the requirements of this

49 CFR Ch. I (10-1-05 Edition)

subchapter and have the appropriate State-issued commercial driver's license required by 49 CFR part 383. Specialized training shall include the following:

- (1) Operation of emergency control features of the cargo tank or portable tank;
- (2) Special vehicle handling characteristics, including: high center of gravity, fluid-load subject to surge, effects of fluid-load surge on braking, characteristic differences in stability among baffled, unbaffled, and multi-compartmented tanks; and effects of partial loads on vehicle stability;
- (3) Loading and unloading procedures;
- (4) The properties and hazards of the material transported; and
- (5) Retest and inspection requirements for cargo tanks.

(c) The training required by paragraphs (a) and (b) of this section may be satisfied by compliance with the current requirements for a Commercial Driver's License (CDL) with a tank vehicle or hazardous materials endorsement.

(d) Training required by paragraph (b) of this section must conform to the requirements of §172.704 of this subchapter with respect to frequency and recordkeeping.

[Amdt. 177-79, 57 FR 20954, May 15, 1992, as amended by Amdt. 177-79, 58 FR 5852, Jan. 22, 1993]

§ 177.817 Shipping papers.

(a) *General requirements.* A person may not accept a hazardous material for transportation or transport a hazardous material by highway unless that person has received a shipping paper prepared in accordance with part 172 of this subchapter or the material is excepted from shipping paper requirements under this subchapter. A subsequent carrier may not transport a hazardous material unless it is accompanied by a shipping paper prepared in accordance with part 172 of this subchapter, except for §172.204, which is not required.

(b) *Shipper certification.* An initial carrier may not accept a hazardous material offered for transportation unless the shipping paper describing the

material includes a shipper's certification which meets the requirements in §172.204 of this subchapter. Except for a hazardous waste, the certification is not required for shipments to be transported entirely by private carriage and for bulk shipments to be transported in a cargo tank supplied by the carrier.

(c) *Requirements when interlining with carriers by rail.* A motor carrier shall mark on the shipping paper required by this section, if it offers or delivers a freight container or transport vehicle to a rail carrier for further transportation:

(1) A description of the freight container or transport vehicle; and

(2) The kind of placard affixed to the freight container or transport vehicle.

(d) This subpart does not apply to a material that is excepted from shipping paper requirements as specified in §172.200 of this subchapter.

(e) *Shipping paper accessibility—accident or inspection.* A driver of a motor vehicle containing hazardous material, and each carrier using such a vehicle, shall ensure that the shipping paper required by this section is readily available to, and recognizable by, authorities in the event of accident or inspection. Specifically, the driver and the carrier shall:

(1) Clearly distinguish the shipping paper, if it is carried with other shipping papers or other papers of any kind, by either distinctively tabbing it or by having it appear first; and

(2) Store the shipping paper as follows:

(i) When the driver is at the vehicle's controls, the shipping paper shall be: (A) Within his immediate reach while he is restrained by the lap belt; and (B) either readily visible to a person entering the driver's compartment or in a holder which is mounted to the inside of the door on the driver's side of the vehicle.

(ii) When the driver is not at the vehicle's controls, the shipping paper shall be: (A) In a holder which is mounted to the inside of the door on the driver's side of the vehicle; or (B) on the driver's seat in the vehicle.

(f) *Retention of shipping papers.* Each person receiving a shipping paper required by this section must retain a

copy or an electronic image thereof, that is accessible at or through its principal place of business and must make the shipping paper available, upon request, to an authorized official of a Federal, State, or local government agency at reasonable times and locations. For a hazardous waste, the shipping paper copy must be retained for three years after the material is accepted by the initial carrier. For all other hazardous materials, the shipping paper copy must be retained for 375 days after the material is accepted by the carrier. Each shipping paper copy must include the date of acceptance by the carrier. A motor carrier (as defined in §390.5 of subchapter B of chapter III of subtitle B) using a shipping paper without change for multiple shipments of one or more hazardous materials having the same shipping name and identification number may retain a single copy of the shipping paper, instead of a copy for each shipment made, if the carrier also retains a record of each shipment made that includes shipping name, identification number, quantity transported, and date of shipment.

[Amdt. 177-35, 41 FR 16130, Apr. 15, 1976, as amended by Amdt. 177-35A, 41 FR 40691, Sept. 20, 1976; Amdt. 177-48, 45 FR 47670, Nov. 10, 1980; Amdt. 177-65, 50 FR 11055, Mar. 19, 1985; Amdt. 177-72, 53 FR 17160, May 13, 1988; 67 FR 46128, July 12, 2002; 67 FR 66574, Nov. 1, 2002; 68 FR 19277, Apr. 18, 2003; 68 FR 57633, Oct. 6, 2003]

§ 177.823 Movement of motor vehicles in emergency situations.

(a) A carrier may not move a transport vehicle containing a hazardous material unless the vehicle is marked and placarded in accordance with part 172 or as authorized in §171.12a of this subchapter, or unless, in an emergency:

(1) The vehicle is escorted by a representative of a state or local government;

(2) The carrier has permission from the Department; or

(3) Movement of the transport vehicle is necessary to protect life or property.

(b) *Disposition of contents of cargo tank when unsafe to continue.* In the event of a leak in a cargo tank of such a character as to make further transportation unsafe, the leaking vehicle should be removed from the traveled

portion of the highway and every available means employed for the safe disposal of the leaking material by preventing, so far as practicable, its spread over a wide area, such as by digging trenches to drain to a hole or depression in the ground, diverting the liquid away from streams or sewers if possible, or catching the liquid in containers if practicable. Smoking, and any other source of ignition, in the vicinity of a leaking cargo tank is not permitted.

(c) *Movement of leaking cargo tanks.* A leaking cargo tank may be transported only the minimum distance necessary to reach a place where the contents of the tank or compartment may be disposed of safely. Every available means must be utilized to prevent the leakage or spillage of the liquid upon the highway.

[Amdt. 177-35, 41 FR 16130, Apr. 15, 1976, as amended by Amdt. 177-67, 50 FR 41521, Oct. 11, 1985; Amdt. 177-86, 61 FR 18933, Apr. 29, 1996]

Subpart B—Loading and Unloading

NOTE: For prohibited loading and storage of hazardous materials, see § 177.848.

§ 177.834 General requirements.

(a) *Packages secured in a motor vehicle.* Any package containing any hazardous material, not permanently attached to a motor vehicle, must be secured against shifting, including relative motion between packages, within the vehicle on which it is being transported, under conditions normally incident to transportation. Packages having valves or other fittings must be loaded in a manner to minimize the likelihood of damage during transportation.

(b) Each package containing a hazardous material bearing package orientation markings prescribed in § 172.312 of this subchapter must be loaded on a transport vehicle or within a freight container in accordance with such markings and must remain in the correct position indicated by the markings during transportation.

(c) *No smoking while loading or unloading.* Smoking on or about any motor vehicle while loading or unloading any Class 1 (explosive), Class 3 (flammable

liquid), Class 4 (flammable solid), Class 5 (oxidizing), or Division 2.1 (flammable gas) materials is forbidden.

(d) *Keep fire away, loading and unloading.* Extreme care shall be taken in the loading or unloading of any Class 1 (explosive), Class 3 (flammable liquid), Class 4 (flammable solid), Class 5 (oxidizing), or Division 2.1 (flammable gas) materials into or from any motor vehicle to keep fire away and to prevent persons in the vicinity from smoking, lighting matches, or carrying any flame or lighted cigar, pipe, or cigarette.

(e) *Handbrake set while loading and unloading.* No hazardous material shall be loaded into or on, or unloaded from, any motor vehicle unless the handbrake be securely set and all other reasonable precautions be taken to prevent motion of the motor vehicle during such loading or unloading process.

(f) *Use of tools, loading and unloading.* No tools which are likely to damage the effectiveness of the closure of any package or other container, or likely adversely to affect such package or container, shall be used for the loading or unloading of any Class 1 (explosive) material or other dangerous article.

(g) [Reserved]

(h) *Precautions concerning containers in transit; fueling road units.* Reasonable care should be taken to prevent undue rise in temperature of containers and their contents during transit. There must be no tampering with such container or the contents thereof nor any discharge of the contents of any container between point of origin and point of billed destination. Discharge of contents of any container, other than a cargo tank or IM portable tank, must not be made prior to removal from the motor vehicle. Nothing contained in this paragraph shall be so construed as to prohibit the fueling of machinery or vehicles used in road construction or maintenance.

(i) *Attendance requirements.* (1) *Loading.* A cargo tank must be attended by a qualified person at all times when it is being loaded. The person who is responsible for loading the cargo tank is also responsible for ensuring that it is so attended.

(2) *Unloading.* A motor carrier who transports hazardous materials by a

Title 49: Transportation

PART 383—COMMERCIAL DRIVER'S LICENSE STANDARDS; REQUIREMENTS AND PENALTIES

Subpart B—Single License Requirement

§ 383.21 Number of drivers' licenses.

No person who operates a commercial motor vehicle shall at any time have more than one driver's license.

[64 FR 48110, Sept. 2, 1999]

§ 383.23 Commercial driver's license.

(a) *General rule.* (1) Effective April 1, 1992, no person shall operate a commercial motor vehicle unless such person has taken and passed written and driving tests which meet the Federal standards contained in subparts F, G, and H of this part for the commercial motor vehicle that person operates or expects to operate.

(2) Except as provided in paragraph (b) of this section, no person may legally operate a CMV unless such person possesses a CDL which meets the standards contained in subpart J of this part, issued by his/her State or jurisdiction of domicile.

(b) *Exception.* (1) If a CMV operator is not domiciled in a foreign jurisdiction which the Administrator has determined tests drivers and issues CDLs in accordance with, or under standards similar to, the standards contained in subparts F, G, and H of this part, the person may obtain a Nonresident CDL from a State which does comply with the testing and licensing standards contained in such subparts F, G, and H of this part.¹

¹ Effective December 29, 1988, the Administrator determined that commercial drivers' licensees issued by Canadian Provinces and Territories in conformity with the Canadian National Safety Code are in accordance with the standards of this part. Effective November 21, 1991, the Administrator determined that the new Licencias Federales de Conductor issued by the United Mexican States are in accordance with the standards of this part. Therefore, under the single license provision of §383.21, a driver holding a commercial driver's license issued under the Canadian National Safety Code or a new Licencia Federal de Conductor issued by Mexico is prohibited from obtaining nonresident CDL, or any other type of driver's license, from a State or other jurisdiction in the United States.

(2) If an individual is domiciled in a State while that State is prohibited from issuing CDLs in accordance with §384.405 of this subchapter, that individual is eligible to obtain a Nonresident CDL from any State that elects to issue a Nonresident CDL and which complies with the testing and licensing standards contained in subparts F, G, and H of this part.

(c) *Learner's permit.* State learners' permits, issued for limited time periods according to State requirements, shall be considered valid commercial drivers' licenses for purposes of behind-the-wheel training on public roads or highways, if the following minimum conditions are met:

(1) The learner's permit holder is at all times accompanied by the holder of a valid CDL;

(2) He/she either holds a valid automobile driver's license, or has passed such vision, sign/symbol, and knowledge tests as the State issuing the learner's permit ordinarily administers to applicants for automotive drivers' licenses; and

(3) He/she does not operate a commercial motor vehicle transporting hazardous materials as defined in §383.5.

[53 FR 27649, July 21, 1988, as amended at 54 FR 22285, May 23, 1989; 57 FR 31457, July 16, 1992; 67 FR 49756, July 31, 2002; 68 FR 23849, May 5, 2003]

[Code of Federal Regulations]

[Title 49, Volume 5]

[Revised as of October 1, 2006]

From the U.S. Government Printing Office via GPO Access

[CITE: 49CFR383.121]

[Page 206]

TITLE 49--TRANSPORTATION

CHAPTER III--FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION,

DEPARTMENT OF TRANSPORTATION

PART 383_COMMERCIAL DRIVER'S LICENSE STANDARDS; REQUIREMENTS AND PENALTIES--Table of

Subpart G_Required Knowledge and Skills

Sec. 383.121 Requirements for hazardous materials endorsement.

In order to obtain a Hazardous Material Endorsement each applicant must have such knowledge as is required of a driver of a hazardous materials laden vehicle, from information contained in 49 CFR parts 171, 172, 173, 177, 178, and 397 on the following:

- (a) Hazardous materials regulations including:
 - (1) Hazardous materials table;
 - (2) Shipping paper requirements;
 - (3) Marking;
 - (4) Labeling;

- (5) Placarding requirements;
 - (6) Hazardous materials packaging;
 - (7) Hazardous materials definitions and preparation;
 - (8) Other regulated material (e.g., ORM-D);
 - (9) Reporting hazardous materials accidents; and
 - (10) Tunnels and railroad crossings.
- (b) Hazardous materials handling including:
- (1) Forbidden Materials and Packages;
 - (2) Loading and Unloading Materials;
 - (3) Cargo Segregation;
 - (4) Passenger Carrying Buses and Hazardous Materials;
 - (5) Attendance of Motor Vehicles;
 - (6) Parking;
 - (7) Routes;
 - (8) Cargo Tanks; and
 - (9) ``Safe Havens.''
- (c) Operation of emergency equipment including:
- (1) Use of equipment to protect the public;
 - (2) Special precautions for equipment to be used in fires;
 - (3) Special precautions for use of emergency equipment when loading or unloading a hazardous materials laden motor vehicle; and
 - (4) Use of emergency equipment for tank vehicles.
- (d) Emergency response procedures including:
- (1) Special care and precautions for different types of accidents;
 - (2) Special precautions for driving near a fire and carrying hazardous materials, and smoking and carrying hazardous materials;
 - (3) Emergency procedures; and
 - (4) Existence of special requirements for transporting Class A and B explosives.

[Code of Federal Regulations]

[Title 49, Volume 5]

[Revised as of October 1, 2006]

From the U.S. Government Printing Office via GPO Access

[CITE: 49CFR383.141]

[Page 210-211]

TITLE 49--TRANSPORTATION

CHAPTER III--FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION,

DEPARTMENT OF TRANSPORTATION

PART 383_COMMERCIAL DRIVER'S LICENSE STANDARDS; REQUIREMENTS AND
PENALTIES--Table of Contents

Subpart I_Requirement for Transportation Security Administration
approval of hazardous materials endorsement issuances

Sec. 383.141 General.

(a) Applicability date. Beginning on the date(s) listed in 49 CFR 1572.13(b), this section applies to State agencies responsible for issuing hazardous materials endorsements for a CDL, and applicants for such endorsements.

(b) Prohibition. A State may not issue, renew, upgrade, or transfer

a hazardous materials endorsement for a CDL to any individual authorizing that individual to operate a commercial motor vehicle transporting a hazardous material in commerce unless the Transportation Security Administration has determined that the individual does not pose a security risk warranting denial of the endorsement.

(c) Individual notification. At least 60 days prior to the expiration date of the CDL or hazardous materials endorsement, a State must notify the holder of a hazardous materials endorsement that the individual must pass a Transportation Security Administration security threat assessment process as part of any application for renewal of the hazardous materials endorsement. The notice must advise a driver that, in order to expedite the security

[[Page 211]]

screening process, he or she should file a renewal application as soon as possible, but not later than 30 days before the date of expiration of the endorsement. An individual who does not successfully complete the Transportation Security Administration security threat assessment process referenced in paragraph (b) of this section may not be issued a hazardous materials endorsement.

(d) Hazardous materials endorsement renewal cycle. Each State must require that hazardous materials endorsements be renewed every 5 years or less so that individuals are subject to a Transportation Security Administration security screening requirement referenced in paragraph (b) of this section at least every 5 years.

FR 51393, Aug. 19, 2004; 70 FR 22271, Apr. 29, 2005]

§ 391.21

substance, an amphetamine, a narcotic drug, a formulation of an amphetamine, or a derivative of a narcotic drug;

(iii) Transportation, possession, or unlawful use of a 21 CFR 1308.11 *Schedule I* identified controlled substance, amphetamines, narcotic drugs, formulations of an amphetamine, or derivatives of narcotic drugs while the driver is on duty, as the term on-duty time is defined in § 395.2 of this subchapter;

(iv) Leaving the scene of an accident while operating a commercial motor vehicle; or

(v) A felony involving the use of a commercial motor vehicle.

(3) *Duration of disqualification*—(i) *First offenders*. A driver is disqualified for 1 year after the date of conviction or forfeiture of bond or collateral if, during the 3 years preceding that date, the driver was not convicted of, or did not forfeit bond or collateral upon a charge of an offense that would disqualify the driver under the rules of this section. Exemption. The period of disqualification is 6 months if the conviction or forfeiture of bond or collateral solely concerned the transportation or possession of substances named in paragraph (c)(2)(iii) of this section.

(ii) *Subsequent offenders*. A driver is disqualified for 3 years after the date of his/her conviction or forfeiture of bond or collateral if, during the 3 years preceding that date, he/she was convicted of, or forfeited bond or collateral upon a charge of, an offense that would disqualify him/her under the rules in this section.

(d) *Disqualification for violation of out-of-service orders*—(1) *General rule*. A driver who is convicted of violating an out-of-service order is disqualified for the period of time specified in paragraph (d)(2) of this section.

(2) *Duration of disqualification for violation of out-of-service orders*—(i) *First violation*. A driver is disqualified for not less than 90 days nor more than one year if the driver is convicted of a first violation of an out-of-service order.

(ii) *Second violation*. A driver is disqualified for not less than one year nor more than five years if, during any 10-year period, the driver is convicted of two violations of out-of-service orders in separate incidents.

49 CFR Ch. III (10–1–06 Edition)

(iii) *Third or subsequent violation*. A driver is disqualified for not less than three years nor more than five years if, during any 10-year period, the driver is convicted of three or more violations of out-of-service orders in separate incidents.

(iv) *Special rule for hazardous materials and passenger offenses*. A driver is disqualified for a period of not less than 180 days nor more than two years if the driver is convicted of a first violation of an out-of-service order while transporting hazardous materials required to be placarded under the Hazardous Materials Transportation Act (49 U.S.C. 5101 *et seq.*), or while operating commercial motor vehicles designed to transport more than 15 passengers, including the driver. A driver is disqualified for a period of not less than three years nor more than five years if, during any 10-year period, the driver is convicted of any subsequent violations of out-of-service orders, in separate incidents, while transporting hazardous materials required to be placarded under the Hazardous Materials Transportation Act, or while operating commercial motor vehicles designed to transport more than 15 passengers, including the driver.

[37 FR 24902, Nov. 23, 1972, as amended at 49 FR 44215, Nov. 5, 1984; 51 FR 8200, Mar. 10, 1986; 53 FR 18057, May 19, 1988; 53 FR 39051, Oct. 4, 1988; 54 FR 40788, Oct. 3, 1989; 59 FR 26028, May 18, 1994; 60 FR 38744, 38745, July 28, 1995; 62 FR 37152, July 11, 1997; 63 FR 33277, June 18, 1998]

Subpart C—Background and Character

§ 391.21 Application for employment.

(a) Except as provided in subpart G of this part, a person shall not drive a commercial motor vehicle unless he/she has completed and furnished the motor carrier that employs him/her with an application for employment that meets the requirements of paragraph (b) of this section.

(b) The application for employment shall be made on a form furnished by the motor carrier. Each application form must be completed by the applicant, must be signed by him/her, and must contain the following information:

Federal Motor Carrier Safety Administration, DOT

§ 391.23

(1) The name and address of the employing motor carrier;

(2) The applicant's name, address, date of birth, and social security number;

(3) The addresses at which the applicant has resided during the 3 years preceding the date on which the application is submitted;

(4) The date on which the application is submitted;

(5) The issuing State, number, and expiration date of each unexpired commercial motor vehicle operator's license or permit that has been issued to the applicant;

(6) The nature and extent of the applicant's experience in the operation of motor vehicles, including the type of equipment (such as buses, trucks, truck tractors, semitrailers, full trailers, and pole trailers) which he/she has operated;

(7) A list of all motor vehicle accidents in which the applicant was involved during the 3 years preceding the date the application is submitted, specifying the date and nature of each accident and any fatalities or personal injuries it caused;

(8) A list of all violations of motor vehicle laws or ordinances (other than violations involving only parking) of which the applicant was convicted or forfeited bond or collateral during the 3 years preceding the date the application is submitted;

(9) A statement setting forth in detail the facts and circumstances of any denial, revocation, or suspension of any license, permit, or privilege to operate a motor vehicle that has been issued to the applicant, or a statement that no such denial, revocation, or suspension has occurred;

(10)(i) A list of the names and addresses of the applicant's employers during the 3 years preceding the date the application is submitted,

(ii) The dates he or she was employed by that employer,

(iii) The reason for leaving the employ of that employer,

(iv) After October 29, 2004, whether the (A) Applicant was subject to the FMCSRs while employed by that previous employer,

(B) Job was designated as a safety sensitive function in any DOT regu-

lated mode subject to alcohol and controlled substances testing requirements as required by 49 CFR part 40;

(11) For those drivers applying to operate a commercial motor vehicle as defined by Part 383 of this subchapter, a list of the names and addresses of the applicant's employers during the 7-year period preceding the 3 years contained in paragraph (b)(10) of this section for which the applicant was an operator of a commercial motor vehicle, together with the dates of employment and the reasons for leaving such employment; and

(12) The following certification and signature line, which must appear at the end of the application form and be signed by the applicant:

This certifies that this application was completed by me, and that all entries on it and information in it are true and complete to the best of my knowledge.

(Date)

(Applicant's signature)

(c) A motor carrier may require an applicant to provide information in addition to the information required by paragraph (b) of this section on the application form.

(d) Before an application is submitted, the motor carrier must inform the applicant that the information he/she provides in accordance with paragraph (b)(10) of this section may be used, and the applicant's previous employers will be contacted, for the purpose of investigating the applicant's safety performance history information as required by paragraphs (d) and (e) of §391.23. The prospective employer must also notify the driver in writing of his/her due process rights as specified in §391.23(i) regarding information received as a result of these investigations.

[35 FR 6460, Apr. 22, 1970, as amended at 35 FR 17420, Nov. 13, 1970; 52 FR 20589, June 1, 1987; 60 FR 38744, July 28, 1995; 69 FR 16719, Mar. 30, 2004]

§ 391.23 Investigation and inquiries.

(a) Except as provided in subpart G of this part, each motor carrier shall make the following investigations and inquiries with respect to each driver it employs, other than a person who has

Subpart D—Use of Lighted Lamps and Reflectors

§§ 392.30–392.32 [Reserved]

§ 392.33 Obscured lamps or reflective devices/material.

(a) No commercial motor vehicle shall be driven when any of the lamps or reflective devices/material required by subpart B of part 393 of this title are obscured by the tailboard, or by any part of the load or its covering, by dirt, or other added vehicle or work equipment or otherwise.

(b) *Exception.* The conspicuity treatments on the front end protection devices of the trailer may be obscured by part of the load being transported.

[70 FR 48025, Aug. 15, 2005]

Subpart E—License Revocation; Duties of Driver

§§ 392.40–392.41 [Reserved]

Subpart F—Fueling Precautions**§ 392.50 Ignition of fuel; prevention.**

No driver or any employee of a motor carrier shall:

(a) Fuel a commercial motor vehicle with the engine running, except when it is necessary to run the engine to fuel the commercial motor vehicle;

(b) Smoke or expose any open flame in the vicinity of a commercial motor vehicle being fueled;

(c) Fuel a commercial motor vehicle unless the nozzle of the fuel hose is continuously in contact with the intake pipe of the fuel tank;

(d) Permit, insofar as practicable, any other person to engage in such activities as would be likely to result in fire or explosion.

[33 FR 19732, Dec. 25, 1968, as amended at 60 FR 38747, July 28, 1995]

§ 392.51 Reserve fuel; materials of trade.

Small amounts of fuel for the operation or maintenance of a commercial motor vehicle (including its auxiliary equipment) may be designated as materials of trade (see 49 CFR 171.8).

(a) The aggregate gross weight of all materials of trade on a motor vehicle may not exceed 200 kg (440 pounds).

(b) Packaging for gasoline must be made of metal or plastic and conform to requirements of 49 CFR Parts 171, 172, 173, and 178 or requirements of the Occupational Safety and Health Administration contained in 29 CFR 1910.106.

(c) For Packing Group II (including gasoline), Packing Group III (including aviation fuel and fuel oil), or ORM-D, the material is limited to 30 kg (66 pounds) or 30 L (8 gallons).

(d) For diesel fuel, the capacity of the package is limited to 450 L (119 gallons).

(e) A Division 2.1 material in a cylinder is limited to a gross weight of 100 kg (220 pounds). (A Division 2.1 material is a flammable gas, including liquefied petroleum gas, butane, propane, liquefied natural gas, and methane).

[63 FR 33279, June 18, 1998]

§ 392.52 [Reserved]

Subpart G—Prohibited Practices**§ 392.60 Unauthorized persons not to be transported.**

(a) Unless specifically authorized in writing to do so by the motor carrier under whose authority the commercial motor vehicle is being operated, no driver shall transport any person or permit any person to be transported on any commercial motor vehicle other than a bus. When such authorization is issued, it shall state the name of the person to be transported, the points where the transportation is to begin and end, and the date upon which such authority expires. No written authorization, however, shall be necessary for the transportation of:

(1) Employees or other persons assigned to a commercial motor vehicle by a motor carrier;

(2) Any person transported when aid is being rendered in case of an accident or other emergency;

(3) An attendant delegated to care for livestock.

(b) This section shall not apply to the operation of commercial motor vehicles controlled and operated by any farmer and used in the transportation

§ 392.61

of agricultural commodities or products thereof from his/her farm or in the transportation of supplies to his/her farm.

[60 FR 38747, July 28, 1995]

§ 392.61 [Reserved]**§ 392.62 Safe operation, buses.**

No person shall drive a bus and a motor carrier shall not require or permit a person to drive a bus unless—

(a) All standees on the bus are rearward of the standee line or other means prescribed in § 393.90 of this subchapter;

(b) All aisle seats in the bus conform to the requirements of § 393.91 of this subchapter; and

(c) Baggage or freight on the bus is stowed and secured in a manner which assures—

(1) Unrestricted freedom of movement to the driver and his proper operation of the bus;

(2) Unobstructed access to all exits by any occupant of the bus; and

(3) Protection of occupants of the bus against injury resulting from the falling or displacement of articles transported in the bus.

[63 FR 33278, June 18, 1998]

§ 392.63 Towing or pushing loaded buses.

No disabled bus with passengers aboard shall be towed or pushed; nor shall any person use or permit to be used a bus with passengers aboard for the purpose of towing or pushing any disabled motor vehicle, except in such circumstances where the hazard to passengers would be increased by observance of the foregoing provisions of this section, and then only in traveling to the nearest point where the safety of the passengers is assured.

[33 FR 19732, Dec. 25, 1968, as amended at 60 FR 38747, July 28, 1995]

§ 392.64 Riding within closed commercial motor vehicles without proper exits.

No person shall ride within the closed body of any commercial motor vehicle unless there are means on the inside thereof of obtaining exit. Said means

shall be in such condition as to permit ready operation by the occupant.

[33 FR 19732, Dec. 25, 1968, as amended at 60 FR 38747, July 28, 1995]

§ 392.65 [Reserved]**§ 392.66 Carbon monoxide; use of commercial motor vehicle when detected.**

(a) No person shall dispatch or drive any commercial motor vehicle or permit any passengers thereon, when the following conditions are known to exist, until such conditions have been remedied or repaired:

(1) Where an occupant has been affected by carbon monoxide;

(2) Where carbon monoxide has been detected in the interior of the commercial motor vehicle;

(3) When a mechanical condition of the commercial motor vehicle is discovered which would be likely to produce a hazard to the occupants by reason of carbon monoxide.

(b) [Reserved]

[60 FR 38747, July 28, 1995]

§ 392.67 Heater, flame-producing; on commercial motor vehicle in motion.

No open flame heater used in the loading or unloading of the commodity transported shall be in operation while the commercial motor vehicle is in motion.

[33 FR 19732, Dec. 25, 1968, as amended at 60 FR 38747, July 28, 1995]

§§ 392.68–392.69 [Reserved]**§ 392.71 Radar detectors; use and/or possession.**

(a) No driver shall use a radar detector in a commercial motor vehicle, or operate a commercial motor vehicle that is equipped with or contains any radar detector.

(b) No motor carrier shall require or permit a driver to violate paragraph (a) of this section.

[58 FR 67375, Dec. 21, 1993]

training program designed to train students in brake maintenance or inspection similar to the assigned brake service or inspection tasks; or

(B) Experience performing brake maintenance or inspection similar to the assigned brake service or inspection task in a motor carrier maintenance program; or

(C) Experience performing brake maintenance or inspection similar to the assigned brake service or inspection task at a commercial garage, fleet leasing company, or similar facility.

(e) No motor carrier shall employ any person as a brake inspector unless the evidence of the inspector's qualifications, required under this section is maintained by the motor carrier at its principal place of business, or at the location at which the brake inspector is employed. The evidence must be maintained for the period during which the brake inspector is employed in that capacity and for one year thereafter. However, motor carriers do not have to maintain evidence of qualifications to inspect air brake systems for such inspections performed by persons who have passed the air brake knowledge and skills test for a Commercial Driver's License.

[56 FR 491, Jan. 7, 1991]

PART 397—TRANSPORTATION OF HAZARDOUS MATERIALS; DRIVING AND PARKING RULES

Subpart A—General

Sec.

- 397.1 Application of the rules in this part.
- 397.2 Compliance with Federal motor carrier safety regulations.
- 397.3 State and local laws, ordinances, and regulations.
- 397.5 Attendance and surveillance of motor vehicles.
- 397.7 Parking.
- 397.9 [Reserved]
- 397.11 Fires.
- 397.13 Smoking.
- 397.15 Fueling.
- 397.17 Tires.
- 397.19 Instructions and documents.

Subpart B [Reserved]

Subpart C—Routing of Non-Radioactive Hazardous Materials

- 397.61 Purpose and scope.
- 397.63 Applicability.
- 397.65 Definitions.
- 397.67 Motor carrier responsibility for routing.
- 397.69 Highway routing designations; preemption.
- 397.71 Federal standards.
- 397.73 Public information and reporting requirements.
- 397.75 Dispute resolution.
- 397.77 Judicial review of dispute decision.

Subpart D—Routing of Class 7 (Radioactive) Materials

- 397.101 Requirements for motor carriers and drivers.
- 397.103 Requirements for State routing designations.

Subpart E—Preemption Procedures

- 397.201 Purpose and scope of the procedures.
- 397.203 Standards for determining preemption.
- 397.205 Preemption application.
- 397.207 Preemption notice.
- 397.209 Preemption processing.
- 397.211 Preemption determination.
- 397.213 Waiver of preemption application.
- 397.215 Waiver notice.
- 397.217 Waiver processing.
- 397.219 Waiver determination and order.
- 397.221 Timeliness.
- 397.223 Petition for reconsideration.
- 397.225 Judicial review.

AUTHORITY: 49 U.S.C. 322; 49 CFR 1.73. Subpart A also issued under 49 U.S.C. 5103, 31136, 31502, and 49 CFR 1.53. Subparts C, D, and E also issued under 49 U.S.C. 5112, 5125.

SOURCE: 36 FR 4876, Mar. 13, 1971, unless otherwise noted.

EDITORIAL NOTE: Nomenclature changes to part 397 appear at 66 FR 49874, Oct. 1, 2001.

Subpart A—General

§ 397.1 Application of the rules in this part.

(a) The rules in this part apply to each motor carrier engaged in the transportation of hazardous materials by a motor vehicle which must be marked or placarded in accordance with § 177.823 of this title and to—

(1) Each officer or employee of the motor carrier who performs supervisory duties related to the transportation of hazardous materials; and

§ 397.2

(2) Each person who operates or who is in charge of a motor vehicle containing hazardous materials.

(b) Each person designated in paragraph (a) of this section must know and obey the rules in this part.

[36 FR 4876, Mar. 13, 1971, as amended at 36 FR 16067, Aug. 19, 1971; 53 FR 18058, May 19, 1988; 60 FR 38749, July 28, 1995]

§ 397.2 Compliance with Federal motor carrier safety regulations.

A motor carrier or other person to whom this part is applicable must comply with the rules in parts 390 through 397, inclusive, of this subchapter when he/she is transporting hazardous materials by a motor vehicle which must be marked or placarded in accordance with § 177.823 of this title.

[37 FR 18080, Sept. 7, 1972]

§ 397.3 State and local laws, ordinances, and regulations.

Every motor vehicle containing hazardous materials must be driven and parked in compliance with the laws, ordinances, and regulations of the jurisdiction in which it is being operated, unless they are at variance with specific regulations of the Department of Transportation which are applicable to the operation of that vehicle and which impose a more stringent obligation or restraint.

§ 397.5 Attendance and surveillance of motor vehicles.

(a) Except as provided in paragraph (b) of this section, a motor vehicle which contains a Division 1.1, 1.2, or 1.3 (explosive) material must be attended at all times by its driver or a qualified representative of the motor carrier that operates it.

(b) The rules in paragraph (a) of this section do not apply to a motor vehicle which contains Division 1.1, 1.2, or 1.3 material if all the following conditions exist—

(1) The vehicle is located on the property of a motor carrier, on the property of a shipper or consignee of the explosives, in a safe haven, or, in the case of a vehicle containing 50 pounds or less of a Division 1.1, 1.2, or 1.3 material, on a construction or survey site; and

(2) The lawful bailee of the explosives is aware of the nature of the explosives

49 CFR Ch. III (10–1–05 Edition)

the vehicle contains and has been instructed in the procedures which must be followed in emergencies; and

(3) The vehicle is within the bailee's unobstructed field of view or is located in a safe haven.

(c) A motor vehicle which contains hazardous materials other than Division 1.1, 1.2, or 1.3, materials, and which is located on a public street or highway, or the shoulder of a public highway, must be attended by its driver. However, the vehicle need not be attended while its driver is performing duties which are incident and necessary to the driver's duties as the operator of the vehicle.

(d) For purposes of this section—

(1) A motor vehicle is attended when the person in charge of the vehicle is on the vehicle, awake, and not in a sleeper berth, or is within 100 feet of the vehicle and has it within his/her unobstructed field of view.

(2) A qualified representative of a motor carrier is a person who—

(i) Has been designated by the carrier to attend the vehicle;

(ii) Is aware of the nature of the hazardous materials contained in the vehicle he/she attends;

(iii) Has been instructed in the procedures he/she must follow in emergencies; and

(iv) Is authorized to move the vehicle and has the means and ability to do so.

(3) A safe haven in an area specifically approved in writing by local, State, or Federal governmental authorities for the parking of unattended vehicles containing Division 1.1, 1.2, or 1.3 materials.

(e) The rules in this section do not relieve the driver from any obligation imposed by law relating to the placing of warning devices when a motor vehicle is stopped on a public street or highway.

[59 FR 63925, Dec. 12, 1994]

§ 397.7 Parking.

(a) A motor vehicle which contains Division 1.1, 1.2, or 1.3 materials must not be parked under any of the following circumstances—

(1) On or within 5 feet of the traveled portion of a public street or highway;

(2) On private property (including premises of fueling or eating facility)

without the knowledge and consent of the person who is in charge of the property and who is aware of the nature of the hazardous materials the vehicle contains; or

(3) Within 300 feet of a bridge, tunnel, dwelling, or place where people work, congregate, or assemble, except for brief periods when the necessities of operation require the vehicle to be parked and make it impracticable to park the vehicle in any other place.

(b) A motor vehicle which contains hazardous materials other than Division 1.1, 1.2, or 1.3 materials must not be parked on or within five feet of the traveled portion of public street or highway except for brief periods when the necessities of operation require the vehicle to be parked and make it impracticable to park the vehicle in any other place.

[59 FR 63925, Dec. 12, 1994]

§ 397.9 [Reserved]

§ 397.11 Fires.

(a) A motor vehicle containing hazardous materials must not be operated near an open fire unless its driver has first taken precautions to ascertain that the vehicle can safely pass the fire without stopping.

(b) A motor vehicle containing hazardous materials must not be parked within 300 feet of an open fire.

§ 397.13 Smoking.

No person may smoke or carry a lighted cigarette, cigar, or pipe on or within 25 feet of—

(a) A motor vehicle which contains Class 1 materials, Class 5 materials, or flammable materials classified as Division 2.1, Class 3, Divisions 4.1 and 4.2; or

(b) An empty tank motor vehicle which has been used to transport Class 3, flammable materials, or Division 2.1 flammable gases, which when so used, was required to be marked or placarded in accordance with the rules in §177.823 of this title.

[59 FR 63925, Dec. 12, 1994]

§ 397.15 Fueling.

When a motor vehicle which contains hazardous materials is being fueled—

(a) Its engine must not be operating; and

(b) A person must be in control of the fueling process at the point where the fuel tank is filled.

§ 397.17 Tires.

(a) A driver must examine each tire on a motor vehicle at the beginning of each trip and each time the vehicle is parked

(b) If, as the result of an examination pursuant to paragraph (a) of this section, or otherwise, a tire is found to be flat, leaking, or improperly inflated, the driver must cause the tire to be repaired, replaced, or properly inflated before the vehicle is driven. However, the vehicle may be driven to the nearest safe place to perform the required repair, replacement, or inflation.

(c) If, as the result of an examination pursuant to paragraph (a) of this section, or otherwise, a tire is found to be overheated, the driver shall immediately cause the overheated tire to be removed and placed at a safe distance from the vehicle. The driver shall not operate the vehicle until the cause of the overheating is corrected.

(d) Compliance with the rules in this section does not relieve a driver from the duty to comply with the rules in §§397.5 and 397.7.

§ 397.19 Instructions and documents.

(a) A motor carrier that transports Division 1.1, 1.2, or 1.3 (explosive) materials must furnish the driver of each motor vehicle in which the explosives are transported with the following documents:

(1) A copy of the rules in this part;

(2) [Reserved]

(3) A document containing instructions on procedures to be followed in the event of accident or delay. The documents must include the names and telephone numbers of persons (including representatives of carriers or shippers) to be contracted, the nature of the explosives being transported, and the precautions to be taken in emergencies such as fires, accidents, or leakages.

(b) A driver who receives documents in accordance with paragraph (a) of this section must sign a receipt for

§ 397.61

49 CFR Ch. III (10–1–05 Edition)

them. The motor carrier shall maintain the receipt for a period of one year from the date of signature.

(c) A driver of a motor vehicle which contains Division 1.1, 1.2, or 1.3 materials must be in possession of, be familiar with, and be in compliance with

(1) The documents specified in paragraph (a) of this section;

(2) The documents specified in § 177.817 of this title; and

(3) The written route plan specified in § 397.67.

[59 FR 63925, Dec. 12, 1994, as amended at 63 FR 33280, June 18, 1998]

Subpart B [Reserved]

Subpart C—Routing of Non-Radioactive Hazardous Materials

SOURCE: 59 FR 51830, Oct. 12, 1994, unless otherwise noted.

§ 397.61 Purpose and scope.

This subpart contains routing requirements and procedures that States and Indian tribes are required to follow if they establish, maintain, or enforce routing designations over which a non-radioactive hazardous material (NRHM) in a quantity which requires placarding may or may not be transported by a motor vehicle. It also provides regulations for motor carriers transporting placarded or marked NRHM and procedures for dispute resolutions regarding NRHM routing designations.

§ 397.63 Applicability.

The provisions of this subpart apply to any State or Indian tribe that establishes, maintains, or enforces any routing designations over which NRHM may or may not be transported by motor vehicle. They also apply to any motor carrier that transports or causes to be transported placarded or marked NRHM in commerce.

§ 397.65 Definitions.

For purposes of this subpart, the following definitions apply:

Administrator. The Federal Motor Carrier Safety Administrator, who is the chief executive of the Federal Motor Carrier Safety Administration,

an agency within the United States Department of Transportation, or his/her designate.

Commerce. Any trade, traffic, or transportation in the United States which:

(1) Is between a place under the jurisdiction of a State or Indian tribe and any place outside of such jurisdiction; or

(2) Is solely within a place under the jurisdiction of a State or Indian tribe but which affects trade, traffic, or transportation described in subparagraph (a).

FMCSA. The Federal Motor Carrier Safety Administration, an agency within the Department of Transportation.

Hazardous material. A substance or material, including a hazardous substance, which has been determined by the Secretary of Transportation to be capable of posing an unreasonable risk to health, safety, or property when transported in commerce, and which has been so designated.

Indian tribe. Has the same meaning as contained in § 4 of the Indian Self-Determination and Education Act, 25 U.S.C. 450b.

Motor carrier. A for-hire motor carrier or a private motor carrier of property. The term includes a motor carrier's agents, officers and representatives as well as employees responsible for hiring, supervising, training, assigning, or dispatching of drivers.

Motor vehicle. Any vehicle, machine, tractor, trailer, or semitrailer propelled or drawn by mechanical power and used upon the highways in the transportation of passengers or property, or any combination thereof.

NRHM. A non-radioactive hazardous material transported by motor vehicle in types and quantities which require placarding, pursuant to Table 1 or 2 of 49 CFR 172.504.

Political subdivision. A municipality, public agency or other instrumentality of one or more States, or a public corporation, board, or commission established under the laws of one or more States.

Radioactive material. Any material having a specific activity greater than 0.002 microcuries per gram (uCi/g), as defined in 49 CFR 173.403.

§ 397.61

49 CFR Ch. III (10–1–05 Edition)

them. The motor carrier shall maintain the receipt for a period of one year from the date of signature.

(c) A driver of a motor vehicle which contains Division 1.1, 1.2, or 1.3 materials must be in possession of, be familiar with, and be in compliance with

(1) The documents specified in paragraph (a) of this section;

(2) The documents specified in § 177.817 of this title; and

(3) The written route plan specified in § 397.67.

[59 FR 63925, Dec. 12, 1994, as amended at 63 FR 33280, June 18, 1998]

Subpart B [Reserved]

Subpart C—Routing of Non-Radioactive Hazardous Materials

SOURCE: 59 FR 51830, Oct. 12, 1994, unless otherwise noted.

§ 397.61 Purpose and scope.

This subpart contains routing requirements and procedures that States and Indian tribes are required to follow if they establish, maintain, or enforce routing designations over which a non-radioactive hazardous material (NRHM) in a quantity which requires placarding may or may not be transported by a motor vehicle. It also provides regulations for motor carriers transporting placarded or marked NRHM and procedures for dispute resolutions regarding NRHM routing designations.

§ 397.63 Applicability.

The provisions of this subpart apply to any State or Indian tribe that establishes, maintains, or enforces any routing designations over which NRHM may or may not be transported by motor vehicle. They also apply to any motor carrier that transports or causes to be transported placarded or marked NRHM in commerce.

§ 397.65 Definitions.

For purposes of this subpart, the following definitions apply:

Administrator. The Federal Motor Carrier Safety Administrator, who is the chief executive of the Federal Motor Carrier Safety Administration,

an agency within the United States Department of Transportation, or his/her designate.

Commerce. Any trade, traffic, or transportation in the United States which:

(1) Is between a place under the jurisdiction of a State or Indian tribe and any place outside of such jurisdiction; or

(2) Is solely within a place under the jurisdiction of a State or Indian tribe but which affects trade, traffic, or transportation described in subparagraph (a).

FMCSA. The Federal Motor Carrier Safety Administration, an agency within the Department of Transportation.

Hazardous material. A substance or material, including a hazardous substance, which has been determined by the Secretary of Transportation to be capable of posing an unreasonable risk to health, safety, or property when transported in commerce, and which has been so designated.

Indian tribe. Has the same meaning as contained in § 4 of the Indian Self-Determination and Education Act, 25 U.S.C. 450b.

Motor carrier. A for-hire motor carrier or a private motor carrier of property. The term includes a motor carrier's agents, officers and representatives as well as employees responsible for hiring, supervising, training, assigning, or dispatching of drivers.

Motor vehicle. Any vehicle, machine, tractor, trailer, or semitrailer propelled or drawn by mechanical power and used upon the highways in the transportation of passengers or property, or any combination thereof.

NRHM. A non-radioactive hazardous material transported by motor vehicle in types and quantities which require placarding, pursuant to Table 1 or 2 of 49 CFR 172.504.

Political subdivision. A municipality, public agency or other instrumentality of one or more States, or a public corporation, board, or commission established under the laws of one or more States.

Radioactive material. Any material having a specific activity greater than 0.002 microcuries per gram (uCi/g), as defined in 49 CFR 173.403.

Routing agency. The State highway agency or other State agency designated by the Governor of that State, or an agency designated by an Indian tribe, to supervise, coordinate, and approve the NRHM routing designations for that State or Indian tribe.

Routing designations. Any regulation, limitation, restriction, curfew, time of travel restriction, lane restriction, routing ban, port-of-entry designation, or route weight restriction, applicable to the highway transportation of NRHM over a specific highway route or portion of a route.

Secretary. The Secretary of Transportation.

State. A State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, the Virgin Islands, American Samoa or Guam.

§ 397.67 Motor carrier responsibility for routing.

(a) A motor carrier transporting NRHM shall comply with NRHM routing designations of a State or Indian tribe pursuant to this subpart.

(b) A motor carrier carrying hazardous materials required to be placarded or marked in accordance with 49 CFR 177.823 and not subject to a NRHM routing designations pursuant to this subpart, shall operate the vehicle over routes which do not go through or near heavily populated areas, places where crowds are assembled, tunnels, narrow streets, or alleys, except where the motor carrier determines that:

(1) There is no practicable alternative;

(2) A reasonable deviation is necessary to reach terminals, points of loading and unloading, facilities for food, fuel, repairs, rest, or a safe haven; or

(3) A reasonable deviation is required by emergency conditions, such as a detour that has been established by a highway authority, or a situation exists where a law enforcement official requires the driver to take an alternative route.

(c) Operating convenience is not a basis for determining whether it is practicable to operate a motor vehicle

in accordance with paragraph (b) of this section.

(d) Before a motor carrier requires or permits a motor vehicle containing explosives in Class 1, Divisions 1.1, 1.2, 1.3, as defined in 49 CFR 173.50 and 173.53 respectively, to be operated, the carrier or its agent shall prepare a written route plan that complies with this section and shall furnish a copy to the driver. However, the driver may prepare the written plan as agent for the motor carrier when the trip begins at a location other than the carrier's terminal.

§ 397.69 Highway routing designations; preemption.

(a) Any State or Indian tribe that establishes or modifies a highway routing designation over which NRHM may or may not be transported on or after November 14, 1994, and maintains or enforces such designation, shall comply with the highway routing standards set forth in § 397.71 of this subpart. For purposes of this subpart, any highway routing designation affecting the highway transportation of NRHM, made by a political subdivision of a State is considered as one made by that State, and all requirements of this subpart apply.

(b) Except as provided in §§ 397.75 and 397.219, a NRHM route designation made in violation of paragraph (a) of this section is preempted pursuant to section 105(b)(4) of the Hazardous Materials Transportation Act (49 U.S.C. app. 1804(b)(4)). This provision shall become effective after November 14, 1996.

(c) A highway routing designation established by a State, political subdivision, or Indian tribe before November 14, 1994 is subject to preemption in accordance with the preemption standards in paragraphs (a)(1) and (a)(2) of § 397.203 of this subpart.

(d) A State, political subdivision, or Indian tribe may petition for a waiver of preemption in accordance with § 397.213 of this part.

§ 397.71 Federal standards.

(a) A State or Indian tribe shall comply with the Federal standards under paragraph (b) of this section when establishing, maintaining or enforcing specific NRHM routing designations

over which NRHM may or may not be transported.

(b) The Federal standards are as follows:

(1) *Enhancement of public safety.* The State or Indian tribe shall make a finding, supported by the record to be developed in accordance with paragraphs (b)(2)(ii) and (b)(3)(iv) of this section, that any NRHM routing designation enhances public safety in the areas subject to its jurisdiction and in other areas which are directly affected by such highway routing designation. In making such a finding, the State or Indian tribe shall consider:

(i) The factors listed in paragraph (b)(9) of this section; and

(ii) The DOT “Guidelines for Applying Criteria to Designate Routes for Transporting Hazardous Materials,” DOT/RSPA/OHMT-89-02, July 1989¹ or its most current version; or an equivalent routing analysis which adequately considers overall risk to the public.

(2) *Public participation.* Prior to the establishment of any NRHM routing designation, the State or Indian tribe shall undertake the following actions to ensure participation by the public in the routing process:

(i) The State or Indian tribe shall provide the public with notice of any proposed NRHM routing designation and a 30-day period in which to comment. At any time during this period or following review of the comments received, the State or Indian tribe shall decide whether to hold a public hearing on the proposed NRHM route designation. The public shall be given 30 days prior notice of the public hearing which shall be conducted as described in paragraph (b)(2)(ii) of this section. Notice for both the comment period and the public hearing, if one is held, shall be given by publication in at least two newspapers of general circulation in the affected area or areas and shall contain a complete description of the proposed routing designation, together with the date, time, and location of any public hearings. Notice for both

the comment period and any public hearing may also be published in the official register of the State.

(ii) If it is determined that a public hearing is necessary, the State or Indian tribe shall hold at least one public hearing on the record during which the public will be afforded the opportunity to present their views and any information or data related to the proposed NRHM routing designation. The State shall make available to the public, upon payment of prescribed costs, copies of the transcript of the hearing, which shall include all exhibits and documents presented during the hearing or submitted for the record.

(3) *Consultation with others.* Prior to the establishment of any NRHM routing designation, the State or Indian tribe shall provide notice to, and consult with, officials of affected political subdivisions, States and Indian tribes, and any other affected parties. Such actions shall include the following:

(i) At least 60 days prior to establishing a routing designation, the State or Indian tribe shall provide notice, in writing, of the proposed routing designation to officials responsible for highway routing in all other affected States or Indian tribes. A copy of this notice may also be sent to all affected political subdivisions. This notice shall request approval, in writing, by those States or Indian tribes, of the proposed routing designations. If no response is received within 60 days from the day of receipt of the notification of the proposed routing designation, the routing designation shall be considered approved by the affected State or Indian tribe.

(ii) The manner in which consultation under this paragraph is conducted is left to the discretion of the State or Indian tribe.

(iii) The State or Indian tribe shall attempt to resolve any concern or disagreement expressed by any consulted official related to the proposed routing designation.

(iv) The State or Indian tribe shall keep a record of the names and addresses of the officials notified pursuant to this section and of any consultation or meeting conducted with these officials or their representatives. Such record shall describe any concern or

¹This document may be obtained from Office of Enforcement and Compliance (MC-PSDECH), Federal Motor Carrier Safety Administration, U.S. Department of Transportation, 400 7th Street, SW., Washington, D.C. 20590-0001.

disagreement expressed by the officials and any action undertaken to resolve such disagreement or address any concern.

(4) *Through routing.* In establishing any NRHM routing designation, the State or Indian tribe shall ensure through highway routing for the transportation of NRHM between adjacent areas. The term “through highway routing” as used in this paragraph means that the routing designation must ensure continuity of movement so as to not impede or unnecessarily delay the transportation of NRHM. The State or Indian tribe shall utilize the procedures established in paragraphs (b)(2) and (b)(3) of this section in meeting these requirements. In addition, the State or Indian tribe shall make a finding, supported by a risk analysis conducted in accordance with paragraph (b)(1) of this section, that the routing designation enhances public safety. If the risk analysis shows—

(i) That the current routing presents at least 50 percent more risk to the public than the deviation under the proposed routing designation, then the proposed routing designation may go into effect.

(ii) That the current routing presents a greater risk but less than 50 percent more risk to the public than the deviation under the proposed routing restriction, then the proposed routing restriction made by a State or Indian tribe shall only go into effect if it does not force a deviation of more than 25 miles or result in an increase of more than 25 percent of that part of a trip affected by the deviation, whichever is shorter, from the most direct route through a jurisdiction as compared to the intended deviation.

(iii) That the current route has the same or less risk to the public than the deviation resulting from the proposed routing designation, then the routing designation shall not be allowed.

(5) *Agreement of other States; burden on commerce.* Any NRHM routing designation which affects another State or Indian tribe shall be established, maintained, or enforced only if:

(i) It does not unreasonably burden commerce, and

(ii) It is agreed to by the affected State or Indian tribe within 60 days of

receipt of the notice sent pursuant to paragraph (b)(3)(i) of this section, or it is approved by the Administrator pursuant to § 397.75.

(6) *Timeliness.* The establishment of a NRHM routing designation by any State or Indian tribe shall be completed within 18 months of the notice given in either paragraph (b)(2) or (b)(3) of this section, whichever occurs first.

(7) *Reasonable routes to terminals and other facilities.* In establishing or providing for reasonable access to and from designated routes, the State or Indian tribe shall use the shortest practicable route considering the factors listed in paragraph (b)(9) of this section. In establishing any NRHM routing designation, the State or Indian tribe shall provide reasonable access for motor vehicles transporting NRHM to reach:

(i) Terminals,

(ii) Points of loading, unloading, pickup and delivery, and

(iii) Facilities for food, fuel, repairs, rest, and safe havens.

(8) *Responsibility for local compliance.* The States shall be responsible for ensuring that all of their political subdivisions comply with the provisions of this subpart. The States shall be responsible for resolving all disputes between such political subdivisions within their jurisdictions. If a State or any political subdivision thereof, or an Indian tribe chooses to establish, maintain, or enforce any NRHM routing designation, the Governor, or Indian tribe, shall designate a routing agency for the State or Indian tribe, respectively. The routing agency shall ensure that all NRHM routing designations within its jurisdiction comply with the Federal standards in this section. The State or Indian tribe shall comply with the public information and reporting requirements contained in § 397.73.

(9) *Factors to consider.* In establishing any NRHM routing designation, the State or Indian tribe shall consider the following factors:

(i) *Population density.* The population potentially exposed to a NRHM release shall be estimated from the density of the residents, employees, motorists, and other persons in the area, using United States census tract maps or

other reasonable means for determining the population within a potential impact zone along a designated highway route. The impact zone is the potential range of effects in the event of a release. Special populations such as schools, hospitals, prisons, and senior citizen homes shall, among other things, be considered when determining the potential risk to the populations along a highway routing. Consideration shall be given to the amount of time during which an area will experience a heavy population density.

(ii) *Type of highway.* The characteristics of each alternative NRHM highway routing designation shall be compared. Vehicle weight and size limits, underpass and bridge clearances, roadway geometrics, number of lanes, degree of access control, and median and shoulder structures are examples of characteristics which a State or Indian tribe shall consider.

(iii) *Types and quantities of NRHM.* An examination shall be made of the type and quantity of NRHM normally transported along highway routes which are included in a proposed NRHM routing designation, and consideration shall be given to the relative impact zone and risks of each type and quantity.

(iv) *Emergency response capabilities.* In consultation with the proper fire, law enforcement, and highway safety agencies, consideration shall be given to the emergency response capabilities which may be needed as a result of a NRHM routing designation. The analysis of the emergency response capabilities shall be based upon the proximity of the emergency response facilities and their capabilities to contain and suppress NRHM releases within the impact zones.

(v) *Results of consultation with affected persons.* Consideration shall be given to the comments and concerns of all affected persons and entities provided during public hearings and consultations conducted in accordance with this section.

(vi) *Exposure and other risk factors.* States and Indian tribes shall define the exposure and risk factors associated with any NRHM routing designations. The distance to sensitive areas shall be considered. Sensitive areas include, but are not limited to, homes

and commercial buildings; special populations in hospitals, schools, handicapped facilities, prisons and stadiums; water sources such as streams and lakes; and natural areas such as parks, wetlands, and wildlife reserves.

(vii) *Terrain considerations.* Topography along and adjacent to the proposed NRHM routing designation that may affect the potential severity of an accident, the dispersion of the NRHM upon release and the control and clean up of NRHM if released shall be considered.

(viii) *Continuity of routes.* Adjacent jurisdictions shall be consulted to ensure routing continuity for NRHM across common borders. Deviations from the most direct route shall be minimized.

(ix) *Alternative routes.* Consideration shall be given to the alternative routes to, or resulting from, any NRHM route designation. Alternative routes shall be examined, reviewed, or evaluated to the extent necessary to demonstrate that the most probable alternative routing resulting from a routing designation is safer than the current routing.

(x) *Effects on commerce.* Any NRHM routing designation made in accordance with this subpart shall not create an unreasonable burden upon interstate or intrastate commerce.

(xi) *Delays in transportation.* No NRHM routing designations may create unnecessary delays in the transportation of NRHM.

(xii) *Climatic conditions.* Weather conditions unique to a highway route such as snow, wind, ice, fog, or other climatic conditions that could affect the safety of a route, the dispersion of the NRHM upon release, or increase the difficulty of controlling it and cleaning it up shall be given appropriate consideration.

(xiii) *Congestion and accident history.* Traffic conditions unique to a highway routing such as: traffic congestion; accident experience with motor vehicles, traffic considerations that could affect the potential for an accident, exposure of the public to any release, ability to perform emergency response operations, or the temporary closing of a highway for cleaning up any release

shall be given appropriate consideration.

§ 397.73 Public information and reporting requirements.

(a) *Public information.* Information on NRHM routing designations must be made available by the States and Indian tribes to the public in the form of maps, lists, road signs or some combination thereof. If road signs are used, those signs and their placements must comply with the provisions of the Manual on Uniform Traffic Control Devices,² published by the FMCSA, particularly the Hazardous Cargo signs identified as R14-2 and R14-3 shown in Section 2B-43 of that Manual.

(b) *Reporting and publishing requirements.* Each State or Indian tribe, through its routing agency, shall provide information identifying all NRHM routing designations which exist within their jurisdictions on November 14, 1994 to the FMCSA, Office of Enforcement and Compliance (MC-PSDECH), 400 7th St., SW., Washington, D.C. 20590-0001 by March 13, 1995. The State or Indian tribe shall include descriptions of these routing designations, along with the dates they were established. This information may also be published in each State's official register of State regulations. Information on any subsequent changes or new NRHM routing designations shall be furnished within 60 days after establishment to the FMCSA. This information will be available from the FMCSA, consolidated by the FMCSA, and published annually in whole or as updates in the FEDERAL REGISTER. Each State may also publish this information in its official register of State regulations.

(Approved by the Office of Management and Budget under control number 2125-0554)

§ 397.75 Dispute resolution.

(a) *Petition.* One or more States or Indian tribes may petition the Administrator to resolve a dispute relating to an agreement on a proposed NRHM routing designation. In resolving a dispute under these provisions, the Administrator will provide the greatest level of safety possible without unreasonably burdening commerce, and ensure compliance with the Federal standards established at § 397.71 of this subpart.

(b) *Filing.* Each petition for dispute resolution filed under this section must:

(1) Be submitted to the Administrator, Federal Motor Carrier Safety Administration, U.S. Department of Transportation, 400 7th Street, SW., Washington, DC 20590-0001. Attention: Office of the Chief Counsel (MC-PSDCC).

(2) Identify the State or Indian tribe filing the petition and any other State, political subdivision, or Indian tribe whose NRHM routing designation is the subject of the dispute.

(3) Contain a certification that the petitioner has complied with the notification requirements of paragraph (c) of this section, and include a list of the names and addresses of each State, political subdivision, or Indian tribe official who was notified of the filing of the petition.

(4) Clearly set forth the dispute for which resolution is sought, including a complete description of any disputed NRHM routing designation and an explanation of how the disputed routing designation affects the petitioner or how it impedes through highway routing. If the routing designation being disputed results in alternative routing, then a comparative risk analysis for the designated route and the resulting alternative routing shall be provided.

(5) Describe any actions taken by the State or Indian tribe to resolve the dispute.

(6) Explain the reasons why the petitioner believes that the Administrator should intervene in resolving the dispute.

(7) Describe any proposed actions that the Administrator should take to resolve the dispute and how these actions would provide the greatest level of highway safety without unreasonably burdening commerce and would

²This publication may be purchased from the Superintendent of Documents, U.S. Government Printing Office (GPO), Washington, D.C. 20402 and has Stock No. 050-001-81001-8. It is available for inspection and copying as prescribed in 49 CFR part 7, appendix D. See 23 CFR part 655, subpart F.

ensure compliance with the Federal standards established in this subpart.

(c) *Notice.* (1) Any State or Indian tribe that files a petition for dispute resolution under this subpart shall mail a copy of the petition to any affected State, political subdivision, or Indian tribe, accompanied by a statement that the State, political subdivision, or Indian tribe may submit comments regarding the petition to the Administrator within 45 days.

(2) By serving notice on any other State, political subdivision, or Indian tribe determined by the Administrator to be possibly affected by the issues in dispute or the resolution sought, or by publication in the FEDERAL REGISTER, the Administrator may afford those persons an opportunity to file written comments on the petition.

(3) Any affected State, political subdivision, or Indian tribe submitting written comments to the Administrator with respect to a petition filed under this section shall send a copy of the comments to the petitioner and certify to the Administrator as to having complied with this requirement. The Administrator may notify other persons participating in the proceeding of the comments and provide an opportunity for those other persons to respond.

(d) *Court actions.* After a petition for dispute resolution is filed in accordance with this section, no court action may be brought with respect to the subject matter of such dispute until a final decision has been issued by the Administrator or until the last day of the one-year period beginning on the day the Administrator receives the petition, whichever occurs first.

(e) *Hearings; alternative dispute resolution.* Upon receipt of a petition filed pursuant to paragraph (a) of this section, the Administrator may schedule a hearing to attempt to resolve the dispute and, if a hearing is scheduled, will notify all parties to the dispute of the date, time, and place of the hearing. During the hearing the parties may offer any information pertinent to the resolution of the dispute. If an agreement is reached, it may be stipulated by the parties, in writing, and, if the Administrator agrees, made part of the decision in paragraph (f) of this sec-

tion. If no agreement is reached, the Administrator may take the matter under consideration and announce his or her decision in accordance with paragraph (f) of this section. Nothing in this section shall be construed as prohibiting the parties from settling the dispute or seeking other methods of alternative dispute resolution prior to the final decision by the Administrator.

(f) *Decision.* The Administrator will issue a decision based on the petition, the written comments submitted by the parties, the record of the hearing, and any other information in the record. The decision will include a written statement setting forth the relevant facts and the legal basis for the decision.

(g) *Record.* The Administrator will serve a copy of the decision upon the petitioner and any other party who participated in the proceedings. A copy of each decision will be placed on file in the public docket. The Administrator may publish the decision or notice of the decision in the FEDERAL REGISTER.

§ 397.77 Judicial review of dispute decision.

Any State or Indian tribe adversely affected by the Administrator's decision under § 397.75 of this subpart may seek review by the appropriate district court of the United States under such proceeding only by filing a petition with such court within 90 days after such decision becomes final.

Subpart D—Routing of Class 7 (Radioactive) Materials

§ 397.101 Requirements for motor carriers and drivers.

(a) Except as provided in paragraph (b) of this section or in circumstances when there is only one practicable highway route available, considering operating necessity and safety, a carrier or any person operating a motor vehicle that contains a Class 7 (radioactive) material, as defined in 49 CFR 172.403, for which placarding is required under 49 CFR part 172 shall:

(1) Ensure that the motor vehicle is operated on routes that minimize radiological risk;

(2) Consider available information on accident rates, transit time, population density and activities, and the time of day and the day of week during which transportation will occur to determine the level of radiological risk; and

(3) Tell the driver which route to take and that the motor vehicle contains Class 7 (radioactive) materials.

(b) Except as otherwise permitted in this paragraph and in paragraph (f) of this section, a carrier or any person operating a motor vehicle containing a highway route controlled quantity of Class 7 (radioactive) materials, as defined in 49 CFR 173.403(l), shall operate the motor vehicle only over preferred routes.

(1) For purposes of this subpart, a preferred route is an Interstate System highway for which an alternative route is not designated by a State routing agency; a State-designated route selected by a State routing agency pursuant to § 397.103; or both of the above.

(2) The motor carrier or the person operating a motor vehicle containing a highway route controlled quantity of Class 7 (radioactive) materials, as defined in 49 CFR 173.403(l) and (y), shall select routes to reduce time in transit over the preferred route segment of the trip. An Interstate System bypass or Interstate System beltway around a city, when available, shall be used in place of a preferred route through a city, unless a State routing agency has designated an alternative route.

(c) A motor vehicle may be operated over a route, other than a preferred route, only under the following conditions:

(1) The deviation from the preferred route is necessary to pick up or deliver a highway route controlled quantity of Class 7 (radioactive) materials, to make necessary rest, fuel or motor vehicle repair stops, or because emergency conditions make continued use of the preferred route unsafe or impossible;

(2) For pickup and delivery not over preferred routes, the route selected must be the shortest-distance route from the pickup location to the nearest preferred route entry location, and the shortest-distance route to the delivery location from the nearest preferred route exit location. Deviation from the

shortest-distance pickup or delivery route is authorized if such deviation:

(i) Is based upon the criteria in paragraph (a) of this section to minimize the radiological risk; and

(ii) Does not exceed the shortest-distance pickup or delivery route by more than 25 miles and does not exceed 5 times the length of the shortest-distance pickup or delivery route.

(iii) Deviations from preferred routes, or pickup or delivery routes other than preferred routes, which are necessary for rest, fuel, or motor vehicle repair stops or because of emergency conditions, shall be made in accordance with the criteria in paragraph (a) of this section to minimize radiological risk, unless due to emergency conditions, time does not permit use of those criteria.

(d) A carrier (or a designated agent) who operates a motor vehicle which contains a package of highway route controlled quantity of Class 7 (radioactive) materials, as defined in 49 CFR 173.403(l), shall prepare a written route plan and supply a copy before departure to the motor vehicle driver and a copy to the shipper (before departure for exclusive use shipments, as defined in 49 CFR 173.403(i), or within fifteen working days following departure for all other shipments). Any variation between the route plan and routes actually used, and the reason for it, shall be reported in an amendment to the route plan delivered to the shipper as soon as practicable but within 30 days following the deviation. The route plan shall contain:

(1) A statement of the origin and destination points, a route selected in compliance with this section, all planned stops, and estimated departure and arrival times; and

(2) Telephone numbers which will access emergency assistance in each State to be entered.

(e) No person may transport a package of highway route controlled quantity of Class 7 (radioactive) materials on a public highway unless:

(1) The driver has received within the two preceding years, written training on:

(i) Requirements in 49 CFR parts 172, 173, and 177 pertaining to the Class 7 (radioactive) materials transported;

§ 397.103

(ii) The properties and hazards of the Class 7 (radioactive) materials being transported; and

(iii) Procedures to be followed in case of an accident or other emergency.

(2) The driver has in his or her immediate possession a certificate of training as evidence of training required by this section, and a copy is placed in his or her qualification file (see § 391.51 of this subchapter), showing:

(i) The driver's name and operator's license number;

(ii) The dates training was provided;

(iii) The name and address of the person providing the training;

(iv) That the driver has been trained in the hazards and characteristics of highway route controlled quantity of Class 7 (radioactive) materials; and

(v) A statement by the person providing the training that information on the certificate is accurate.

(3) The driver has in his or her immediate possession the route plan required by paragraph (d) of this section and operates the motor vehicle in accordance with the route plan.

(f) A person may transport irradiated reactor fuel only in compliance with a plan if required under 49 CFR 173.22(c) that will ensure the physical security of the material. Variation for security purposes from the requirements of this section is permitted so far as necessary to meet the requirements imposed under such a plan, or otherwise imposed by the U.S. Nuclear Regulatory Commission in 10 CFR part 73.

(g) Except for packages shipped in compliance with the physical security requirements of the U.S. Nuclear Regulatory Commission in 10 CFR part 73, each carrier who accepts for transportation a highway route controlled quantity of Class 7 (radioactive) material (see 49 CFR 173.401(1)), must, within 90 days following the acceptance of the package, file the following information concerning the transportation of each such package with the Office of Enforcement and Compliance (MC-PSDECH), Federal Motor Carrier Safety Administration, 400 Seventh Street, SW., Washington, DC 20590-0001:

(1) The route plan required under paragraph (d) of this section, including all required amendments reflecting the routes actually used;

49 CFR Ch. III (10-1-05 Edition)

(2) A statement identifying the names and addresses of the shipper, carrier and consignee; and

(3) A copy of the shipping paper or the description of the Class 7 (radioactive) material in the shipment required by 49 CFR 172.202 and 172.203.

[57 FR 44131, Sept. 24, 1992, as amended at 66 FR 49874, Oct. 1, 2001]

§ 397.103 Requirements for State routing designations.

(a) The State routing agency, as defined in § 397.201(c), shall select routes to minimize radiological risk using "Guidelines for Selecting Preferred Highway Routes for Highway Route Controlled Quantity Shipments of Radioactive Materials," or an equivalent routing analysis which adequately considers overall risk to the public. Designations must be preceded by substantive consultation with affected local jurisdictions and with any other affected States to ensure consideration of all impacts and continuity of designated routes.

(b) State routing agencies may designate preferred routes as an alternative to, or in addition to, one or more Interstate System highways, including interstate system bypasses, or Interstate System beltways.

(c) A State-designated route is effective when—

(1) The State gives written notice by certified mail, return receipt requested, to the Office of Enforcement and Compliance (MC-PSDECH), Attn: National Hazardous Materials Route Registry, 400 Seventh Street, SW., Washington, DC 20590.

(2) Receipt thereof is acknowledged in writing by the FMCSA.

(d) A list of State-designated preferred routes and a copy of the "Guidelines for Selecting Preferred Highway Routes for Highway Route Controlled Quantity Shipments of Radioactive Materials" are available upon request to Office of Enforcement and Compliance (MC-PSDECH), 400 Seventh Street, SW., Washington, DC 20590.

[57 FR 44131, Sept. 24, 1992, as amended at 66 FR 49874, Oct. 1, 2001]

SUBCHAPTER D—MARITIME AND LAND TRANSPORTATION SECURITY

PART 1570—LAND TRANSPORTATION SECURITY: GENERAL RULES

Sec.

1570.1 Scope.

1570.3 Fraud and intentional falsification of records.

AUTHORITY: 49 U.S.C. 114, 40113, 46105.

SOURCE: 68 FR 23869, May 5, 2003, unless otherwise noted.

§ 1570.1 Scope.

This part applies to any person involved in land transportation as specified in this part.

§ 1570.3 Fraud and intentional falsification of records.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with this subchapter, or exercise any privileges under this subchapter.

(b) Any reproduction or alteration, for fraudulent purpose, of any record, report, security program, access medium, or identification medium issued under this subchapter or pursuant to standards in this subchapter.

PART 1572—CREDENTIALING AND BACKGROUND CHECKS FOR LAND TRANSPORTATION SECURITY

Subpart A—Requirements To Undergo Security Threat Assessments

Sec.

1572.1 Applicability.

1572.3 Terms used in this part.

1572.5 Scope and standards for hazardous materials endorsement security threat assessment.

1572.7 Waivers of hazardous materials endorsement security threat assessment standards.

1572.9 Applicant information required for a security threat assessment for a hazardous materials endorsement.

1572.11 Applicant responsibilities for a security threat assessment for a hazardous materials endorsement.

1572.13 State responsibilities for issuance of hazardous materials endorsement.

1572.15 Procedures for security threat assessment.

Subpart B—Standards, Appeals, and Waivers for Security Threat Assessments

1572.101 Scope.

1572.103 Disqualifying criminal offenses.

1572.105 Immigration status.

1572.107 Other analyses.

1572.109 Mental capacity.

1572.111–1572.139 [Reserved]

1572.141 Appeal procedures.

1572.143 Waiver procedures.

Subpart C—Transportation of Explosives From Foreign Locations

1572.201 Transportation of explosives from Canada to the United States via commercial motor vehicle.

1572.203 Transportation of explosives from Canada to the United States via railroad carrier.

Subpart D—Fees for Security Threat Assessments for Individuals

1572.301 Scope and definitions.

1572.303–1572.399 [Reserved]

Subpart E—Fees for Security Threat assessments for Hazmat Drivers

1572.401 Fee collection options.

1572.403 Fee procedures for collection by States.

1572.405 Fee procedures for collection by TSA agents.

AUTHORITY: 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; Sec. 520, Pub. L. 108-90, 117 Stat. 1156 (6 U.S.C. 469)

SOURCE: 69 FR 68742, Nov. 24, 2004, unless otherwise noted.

Subpart A—Requirements To Undergo Security Threat Assessments

§ 1572.1 Applicability.

This part prescribes regulations for credentialing and security threat assessments for certain maritime and land transportation workers.

§ 1572.3 Terms used in this part.

For purposes of this part:

Adjudicate means to make an administrative determination of whether an applicant meets the standards in this part based on the merits of the issues raised.

Alien means any person not a citizen or national of the United States.

Alien registration number means the number issued by the United States Department of Homeland Security to an individual when he or she becomes a lawful permanent resident of the United States or attains other lawful, non-citizen status.

Applicant means an individual who is applying for a new, renewal, or transfer hazardous materials endorsement.

Assistant Secretary means Assistant Secretary for Homeland Security, Transportation Security Administration (Assistant Secretary), who is the highest ranking TSA official, or his or her designee, and who is responsible for making the final determination on the appeal of an intelligence-related check under this part.

Commercial drivers license (CDL) is used as defined in 49 CFR 383.5.

Convicted includes any plea of guilty or *nolo contendere*, or any finding of guilt, except when the finding of guilt is subsequently overturned on appeal, pardoned, or expunged. For purposes of this part, a conviction is expunged when the conviction is removed from the individual's criminal history record and there are no legal disabilities or restrictions associated with the expunged conviction, other than the fact that the conviction may be used for sentencing purposes for subsequent convictions. In addition, where an individual is allowed to withdraw an original plea of guilty or *nolo contendere* and enter a plea of not guilty and the case is subsequently dismissed, the individual is no longer considered to have a conviction for purposes of this part.

Date of service means—

(1) In the case of personal service, the date of personal delivery to the residential address listed on the application;

(2) In the case of mailing with a certificate of service, the date shown on the certificate of service;

(3) In the case of mailing and there is no certificate of service, 10 days from the date mailed to the address designated as the mailing address on the application;

(4) In the case of mailing with no certificate of service or postmark, the date mailed to the address designated as the mailing address on the application shown by other evidence; or

(5) The date on which an electronic transmission occurs.

Day means calendar day.

Determination of No Security Threat means an administrative determination by TSA that an individual does not pose a security threat warranting denial of a hazardous materials endorsement.

Director means the officer designated by the Assistant Secretary to administer the appeal and waiver programs described in this part, except where the Assistant Secretary is specifically designated in this part to administer the appeal or waiver program. The Director may appoint a designee to assume his or her duties.

Endorsement is used as defined in 49 CFR 383.5.

Explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j), and a destructive device as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).

Final Determination of Threat Assessment means a final administrative determination by TSA, including the resolution of related appeals, that an individual poses a security threat warranting denial of a hazardous materials endorsement.

Final Disposition means the actions that must be taken following issuance of a Determination of No Security Threat, a Final Determination of Security Threat, or the grant of a waiver to ensure that a driver's record, a driver's endorsement, and the Commercial Drivers License Information System (CDLIS) accurately reflect the results of the fingerprint and intelligence-related checks.

Firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5845(a) or

§ 1572.5

items contained on the U.S. Munitions Import List at 27 CFR 447.21.

Hazardous material has the same meaning as defined in section 103 of the Hazardous Materials Transportation Act.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, which must be indicated on the individual's commercial driver's license.

Imprisoned or imprisonment means confined to a prison, jail, or institution for the criminally insane, on a full-time basis pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity. Time spent confined or restricted to a half-way house, treatment facility, or similar institution pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity does not constitute imprisonment for purposes of this rule.

Incarceration means confined or otherwise restricted to a jail-type institution, half-way house, treatment facility, or another institution, on a full or part-time basis pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity.

Initial Determination of Threat Assessment means an initial administrative determination by TSA that an individual poses or may pose a security threat warranting denial of a hazardous materials endorsement.

Initial Determination of Threat Assessment and Immediate Revocation means an initial administrative determination that an individual poses a security threat that warrants immediate revocation of an HME. Upon issuance of this document, the State must immediately revoke the hazmat endorsement.

Lawful permanent resident means an individual who has been lawfully admitted to the United States for permanent residence, as defined in 8 U.S.C. 1101.

Mental institution means a mental health facility, mental hospital, sanitarium, psychiatric facility, and any other facility that provides diagnoses by licensed professionals of mental re-

49 CFR Ch. XII (10–1–05 Edition)

tardation or mental illness, including a psychiatric ward in a general hospital.

Pilot State means a State which volunteers to begin the security threat assessment process prior to January 31, 2005.

Revoke means the process by which a State cancels, rescinds, withdraws, or removes a hazardous materials endorsement.

State means a State of the United States and the District of Columbia.

Transportation security incident means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101.

Withdrawal of Initial Determination of Threat Assessment is the document that TSA issues after issuing an Initial Determination of Security Threat, when TSA determines that the applicant does not pose a security threat warranting denial of a hazardous materials endorsement.

§ 1572.5 Scope and standards for hazardous materials endorsement security threat assessment.

(a) This subpart applies to—

(1) State agencies responsible for issuing an HME; and

(2) Applicants who are qualified to hold a commercial driver's license under 49 CFR parts 383 and 384, and are applying for a new, renewal, or transfer HME.

(b) In conducting the security threat assessment requirements in this part, the States and TSA use one or more of the following:

(1) An applicant's fingerprints.

(2) An applicant's name.

(3) Other identifying information.

(c) TSA has determined that an applicant does not pose a security threat warranting denial of an HME if:

(1) The applicant does not have a disqualifying criminal offense described in § 1572.103;

(2) The applicant meets the immigration status requirements described in § 1572.105;

(3) TSA conducts the analyses described in § 1572.107 and determines that the applicant does not pose a security threat; and

(4) The applicant has not been adjudicated as lacking mental capacity or committed to a mental institution, as described in §1572.109.

(d) TSA may direct a State to revoke an individual's HME immediately if TSA determines during the security threat assessment that the individual poses an immediate threat to transportation security, national security or of terrorism.

(e) The regulations of the Federal Motor Carrier Safety Administration (FMCSA) provide that an applicant is disqualified from operating a commercial motor vehicle for specified periods if he or she has an offense that is listed in the FMCSA rules at 49 CFR 383.51. If records indicate that an applicant has committed an offense that would disqualify the applicant from operating a commercial motor vehicle under 49 CFR 383.51, TSA will not issue a Determination of No Security Threat until the State or the FMCSA determine that the applicant is not disqualified under that section.

§1572.7 Waivers of hazardous materials endorsement security threat assessment standards.

(a) An applicant may apply to TSA for a waiver of the standards described in §1572.5, if the applicant—

(1) Has a disqualifying criminal offense described in paragraphs 1572.103(a)(5) through (a)(9), and paragraph 1572.103 (a)(10) if the underlying criminal offense is in paragraphs 1572.103 (a)(5) through (a)(9); or

(2) Has a disqualifying criminal offense described in §1572.103(b); or

(3) Has a history of mental incompetence described in §1572.109.

(b) [Reserved]

§1572.9 Applicant information required for a security threat assessment for a hazardous materials endorsement.

(a) For TSA to complete a security threat assessment, an applicant must supply the information required in this section when the applicant applies to obtain or renew a hazardous materials endorsement. When applying to transfer a hazardous materials endorsement, §1572.13(g) applies.

(b) The application must include the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current mailing address and residential address if it differs from the mailing address; and the previous residential address.

(3) Date of birth.

(4) Social security number.

(5) Gender.

(6) Height, weight, hair and eye color.

(7) City, state, and country of birth.

(8) Immigration status and date of naturalization if the applicant is a naturalized citizen of the United States.

(9) Alien registration number.

(10) State of application, CDL number, and type of endorsement held.

(11) The name, telephone number, and address of the applicant's current employer(s).

(c) The application must include the disqualifying criminal offenses identified in §1572.103.

(d) The application must include a statement, signature, and date of signature that the applicant:

(1) Was not convicted or found not guilty by reason of insanity of a disqualifying crime listed in §1572.103(b) in a civilian or military jurisdiction during the 7 years before the date of the application;

(2) Was not released from incarceration in a civilian or military jurisdiction for committing a disqualifying crime listed in §1572.103(b) during the 5 years before the date of the application;

(3) Is not wanted or under indictment in a civilian or military jurisdiction for a disqualifying criminal offense identified in §1572.103;

(4) Was not convicted or found not guilty by reason of insanity of a disqualifying criminal offense identified in §1572.103(a) in a civilian or military jurisdiction;

(5) Has not been adjudicated as lacking mental capacity or committed to a mental institution involuntarily;

(6) Meets the immigration status requirements described in §1572.105;

(7) Has or has not served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations under §1572.11 impose a

§ 1572.11

49 CFR Ch. XII (10–1–05 Edition)

continuing obligation to disclose to the State within 24 hours if he or she is convicted or found not guilty by reason of insanity of a disqualifying crime, or adjudicated as lacking mental capacity or committed to a mental institution, while he or she holds an HME.

(e) The application must include a statement reading:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 49 U.S.C. 5103a. *Purpose:* This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a hazardous materials endorsement for a commercial drivers license. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will prevent the completion of your security threat assessment, without which you cannot be granted a hazardous materials endorsement. *Routine Uses:* Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact, on this application can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of a hazardous materials endorsement.

§ 1572.11 Applicant responsibilities for a security threat assessment for a hazardous materials endorsement.

(a) *Prohibitions.* An applicant does not meet the security threat assessment standards if he or she:

- (1) Has a disqualifying criminal offense identified in §1572.103, unless TSA grants a waiver under §1572.143; or
- (2) Does not meet the immigration status requirements identified in §1572.105; or
- (3) Has been notified by TSA that he or she poses a security threat under §1572.107; or
- (4) Has been adjudicated as lacking mental capacity or committed to a

mental institution as described in §1572.109, unless TSA grants a waiver under §1572.143.

(b) *Surrender of endorsement.* If an individual is disqualified from holding an HME under paragraph (a) of this section, he or she must surrender the HME and notify TSA. Failure to surrender the HME and notify TSA may result in immediate revocation under §1572.13(a) and/or civil penalties.

(c) *Continuing responsibilities.* An individual who holds an HME must surrender the HME and notify TSA within 24 hours, if he or she:

- (1) Is convicted of, wanted, under indictment, or found not guilty by reason of insanity in a civilian or military jurisdiction for a disqualifying criminal offense identified in §1572.103; or
- (2) Is adjudicated as lacking mental capacity or committed to a mental institution as described in §1572.109; or
- (3) Renounces or loses U.S. citizenship; or
- (4) Violates his or her immigration status and/or is ordered removed from the United States.

(d) *Submission of fingerprints.* (1) An applicant who has not already done so may submit fingerprints in a form and manner specified by TSA when a State revokes the applicant's HME under §1572.13(a).

(2) When so notified by the State, an applicant must submit fingerprints and the information required in §1572.9 in a form and manner specified by the State and TSA, when TSA requests it, or when the applicant applies to obtain or renew an HME. The procedures outlined in §1572.13(g) apply to HME transfers.

(3) When submitting fingerprints and the applicant information required in §1572.9, the applicant or the applicant's employer is responsible for the TSA fee and the FBI fee.

§ 1572.13 State responsibilities for issuance of hazardous materials endorsement.

(a) Each State must immediately revoke an individual's HME if TSA informs the State that the individual does not meet the standards for security threat assessment in §1572.5 and issues an Initial Determination of

Threat Assessment and Immediate Revocation.

(b) Beginning January 31, 2005 for new issuances, and May 31, 2005 for renewal or transfer issuances:

(1) No State may issue or renew a hazardous materials endorsement for a CDL unless the State receives a Determination of No Security Threat from TSA.

(2) Each State must notify each individual holding a hazardous materials endorsement issued by that State that he or she will be subject to the security threat assessment described in this part as part of an application for renewal of the endorsement, at least 60 days prior to the expiration date of the individual's endorsement. The notice must inform the individual that he or she may initiate the security threat assessment required by this section at any time after receiving the notice, but no later than 30 days before the expiration date of the individual's endorsement.

(3) No State may begin processing renewal or transfer applicants prior to March 31, 2005.

(c) Prior to January 31, 2005, as approved by TSA, a Pilot State may not revoke, issue, renew, or transfer a hazardous materials endorsement for a CDL unless the Pilot State—

(1) Collects the information required in §1572.9;

(2) Collects and submits fingerprints in accordance with procedures approved by TSA; and

(3) Receives a Determination of No Security Threat or a Final Determination of Threat Assessment from TSA.

(d) The State that issued an endorsement may extend the expiration date of the endorsement for 90 days if TSA has not provided a Determination of No Security Threat or a Final Determination of Threat Assessment before the expiration date. Any additional extension must be approved in advance by the Director.

(e) Within 15 days of receipt of a Determination of No Security Threat or Final Determination of Threat Assessment from TSA, the State must—

(1) Update the applicant's permanent record to reflect:

(i) The results of the security threat assessment;

(ii) The issuance or denial of an HME; and

(iii) The new expiration date of the HME.

(2) Notify the Commercial Drivers License Information System operator of the results of the security threat assessment.

(3) Revoke or deny the applicant's HME if TSA serves the State with a Final Determination of Threat Assessment.

(f) On or before December 27, 2004, each State must submit a written declaration to TSA, which shall remain in effect until January 31, 2008, unless otherwise authorized by TSA, that states one of the following:

(1) The State elects to collect and submit applicant fingerprints and information, in accordance with the requirements of this part and applicable fingerprint submission standards of the FBI, and the associated TSA and FBI fees; or

(2) The State elects to have TSA/TSA agent collect and submit applicant fingerprints and information, in accordance with the requirements of this part and applicable fingerprint submission standards of the FBI, and the associated TSA and FBI fees. If TSA does not receive a written declaration from a State, TSA will assume responsibility for the collection and submission process.

(g) For applicants who apply to transfer an existing hazardous materials endorsement from one State to another, the second State will not require the applicant to undergo a new security threat assessment until the security threat assessment renewal period established in the preceding issuing State, not to exceed five years, expires.

(h) Each State must retain the application and information required in §1572.9 for at least one year in paper or electronic form.

§ 1572.15 Procedures for security threat assessment.

(a) *Contents of security threat assessment.* The security threat assessment TSA completes includes a fingerprint-based criminal history records check, an intelligence-related background check, and a final disposition.

§ 1572.15

49 CFR Ch. XII (10–1–05 Edition)

(b) *Fingerprint-based check.* In order to conduct a fingerprint-based criminal history records check, the following procedures must be completed:

(1) The State notifies the applicant that he or she will be subject to the security threat assessment at least 60 days prior to the expiration of the applicant's HME and that the applicant must begin the security threat assessment no later than 30 days before the date of the expiration of the HME.

(2) Where the State elects to collect fingerprints and applicant information under § 1572.13(f)(1), the State—

(i) Collects fingerprints and applicant information required in § 1572.9;

(ii) Provides the applicant information to TSA electronically, unless otherwise authorized by TSA;

(iii) Transmits the fingerprints to the FBI/CJIS in accordance with the FBI/CJIS fingerprint submission standards; and

(iv) Retains the signed application, in paper or electronic form, for one year and provides it to TSA if requested.

(3) Where the State elects to have TSA/TSA agent collect fingerprints and applicant information under § 1572.13(f)(2)—

(i) TSA provides a copy of the signed application to the State;

(ii) The State retains the signed application, in paper or electronic form, for one year and provides it to TSA if requested; and

(iii) TSA transmits the fingerprints to the FBI/CJIS in accordance with the FBI/CJIS fingerprint submission standards.

(4) TSA receives the results from the FBI/CJIS and adjudicates the results of the check in accordance with § 1572.103 and, if applicable, § 1572.107.

(c) *Intelligence-related check.* To conduct an intelligence-related check, the following procedures are completed:

(1) TSA reviews the applicant information required in § 1572.9;

(2) TSA searches domestic and international government databases described in §§ 1572.105, 1572.107, and 1572.109;

(3) TSA adjudicates the results of the check in accordance with §§ 1572.103, 1572.105, 1572.107, and 1572.109.

(d) *Final Disposition.* Following completion of the procedures described in

paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the State in which the applicant is authorized to hold an HME, if TSA determines that an applicant meets the security threat assessment standards described in § 1572.5.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses or is suspected of posing a security threat warranting denial of the HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1572.141; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 30 days after receipt of the Initial Determination, or does not request an extension of time within 30 days after receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant and the State, if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5 and may pose an imminent threat to transportation or national security, or of terrorism. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses or is suspected of posing a security threat warranting immediate revocation of an HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1572.141(i); and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 30 days after receipt of the Initial Determination and Immediate Revocation, the Initial Determination

and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) TSA serves a Final Determination of Threat Assessment on the State in which the applicant applied for the HME and on the applicant, if the appeal of the Initial Determination results in a finding that the applicant poses a security threat.

(5) TSA serves a Withdrawal of the Initial Determination of Threat Assessment or a Withdrawal of Final Determination of Threat Assessment on the applicant and a Determination of No Security Threat on the State, if the appeal results in a finding that the applicant does not pose a threat to security, or if TSA grants the applicant a waiver pursuant to § 1572.143.

Subpart B—Standards, Appeals, and Waivers for Security Threat Assessments

§ 1572.101 Scope.

This subpart applies to applicants who hold or are applying to renew or transfer an HME.

§ 1572.103 Disqualifying criminal offenses.

(a) *Permanent disqualifying criminal offenses.* An applicant has a permanent disqualifying offense if convicted or found not guilty by reason of insanity in a civilian or military jurisdiction of any of the following felonies:

- (1) Espionage.
- (2) Sedition.
- (3) Treason.
- (4) A crime listed in 18 U.S.C. Chapter 113B—Terrorism, or a State law that is comparable.
- (5) A crime involving a transportation security incident.
- (6) Improper transportation of a hazardous material under 49 U.S.C. 5124 or a State law that is comparable.
- (7) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device.
- (8) Murder.
- (9) Conspiracy or attempt to commit the crimes in this paragraph (a).
- (10) Violations of the Racketeer Influenced and Corrupt Organizations

Act, 18 U.S.C. 1961, *et seq.*, or a State law that is comparable, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the offenses listed in paragraphs (a)(4) or (a)(8) of this section.

(b) *Interim disqualifying criminal offenses.* The felonies listed in paragraphs (b)(1) through (b)(14) of this section are disqualifying if either of the following factors is true: the applicant was convicted or found not guilty by reason of insanity of the crime in a civilian or military jurisdiction, within the 7 years preceding the date of application; or the applicant was released from incarceration for the crime within the 5 years preceding the date of application.

- (1) Assault with intent to murder.
 - (2) Kidnapping or hostage taking.
 - (3) Rape or aggravated sexual abuse.
 - (4) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon.
 - (5) Extortion.
 - (6) Dishonesty, fraud, or misrepresentation, including identity fraud.
 - (7) Bribery.
 - (8) Smuggling.
 - (9) Immigration violations.
 - (10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, *et seq.*, or a State law that is comparable, other than the violations listed in paragraph (a)(10) of this section.
 - (11) Robbery.
 - (12) Distribution of, possession with intent to distribute, or importation of a controlled substance.
 - (13) Arson.
 - (14) Conspiracy or attempt to commit the crimes in this paragraph (b).
- (c) *Under want or warrant.* An applicant who is wanted or under indictment in any civilian or military jurisdiction for a felony listed in this section is disqualified until the want or warrant is released.
- (d) *Determination of arrest status.* (1) When a fingerprint-based check discloses an arrest for a disqualifying crime listed in this section without indicating a disposition, TSA will so notify the applicant and provide instructions on how the applicant must clear

§ 1572.105

49 CFR Ch. XII (10-1-05 Edition)

the disposition, in accordance with paragraph (d)(2) of this section.

(2) The applicant must provide TSA with written proof that the arrest did not result in a disqualifying criminal offense within 45 days after the service date of the notification in paragraph (d)(1) of this section. If TSA does not receive proof in that time, TSA will notify the applicant and the State that the applicant is disqualified from holding an HME.

§ 1572.105 Immigration status.

(a) An applicant applying for a security threat assessment for an HME must be—

(1) A citizen of the United States who has not renounced or lost his or her United States' citizenship; or

(2) A lawful permanent resident of the United States, as defined in section 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101); or

(3) An individual who is—

(i) In lawful nonimmigrant status and possesses valid evidence of unrestricted employment authorization; or

(ii) A refugee admitted under 8 U.S.C. 1157 and possesses valid evidence of unrestricted employment authorization; or

(iii) An alien granted asylum under 8 U.S.C. 1158, and possesses valid evidence of unrestricted employment authorization.

(b) To determine an applicant's immigration status, TSA checks relevant Federal databases and may perform other checks, including verifying the validity of the applicant's social security number or alien registration number.

§ 1572.107 Other analyses.

(a) An applicant poses a security threat and is therefore disqualified under this section when TSA determines or suspects the applicant of posing a threat—

(1) To national security; or

(2) To transportation security; or

(3) Of terrorism.

(b) TSA checks the following databases and analyzes the resulting information before determining that an applicant does not pose a security threat warranting denial of an HME:

(1) Interpol and other international databases, as appropriate;

(2) Terrorist watchlists and related databases; and

(3) Any other databases relevant to determining whether an applicant poses or is suspected of posing a security threat, or that confirm an applicant's identity.

(c) TSA may determine that an applicant poses a security threat if the search conducted under this part reveals extensive foreign or domestic criminal convictions; a conviction for a serious crime not listed in § 1572.103, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days.

§ 1572.109 Mental capacity.

(a) An applicant has lacking mental capacity if he or she has been—

(1) Adjudicated as lacking mental capacity; or

(2) Committed to a mental institution.

(b) An applicant is adjudicated as lacking mental capacity if—

(1) A court, board, commission, or other lawful authority has determined that the applicant, as a result of marked subnormal intelligence, mental illness, incompetence, condition, or disease, is a danger to him- or herself or others, or lacks the mental capacity to contract or manage his or her own affairs.

(2) This includes a finding of insanity by a court in a criminal case; and a finding of incompetence to stand trial or a finding of not guilty by reason of lack of mental responsibility by any court, or pursuant to articles 50a and 76b of the Uniform Code of Military Justice (10 U.S.C. 850a and 876b).

(c) An applicant is committed to a mental institution if he or she is formally committed to a mental institution by a court, board, commission, or other lawful authority, including involuntary commitment and commitment for lacking mental capacity, mental illness, and drug use. This does not include a commitment to a mental institution for observation or voluntary admission to a mental institution.

§§ 1572.111–1572.139 [Reserved]

§ 1572.141 Appeal procedures.

(a) *Scope.* This section applies to applicants who wish to appeal an Initial Determination of Threat Assessment.

(b) *Grounds for Appeal.* An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she meets the security threat assessment standards identified in §1572.5(c).

(c) *Appeal.* An applicant initiates an appeal by submitting a written reply to TSA or written request for materials from TSA. If the applicant fails to initiate an appeal within 30 days after receipt, the Initial Determination of Threat Assessment becomes final, and TSA serves a Final Determination of Threat Assessment on the State in which the applicant applied.

(1) *Request for materials.* Within 30 days after the date of service of the Initial Determination of Threat Assessment, the applicant may serve upon TSA a written request for copies of the materials upon which the Initial Determination was based.

(2) *TSA response.* (i) Within 30 days after receiving the applicant's request for materials, TSA serves copies of the releasable materials upon the applicant on which the Initial Determination was based. TSA will not include any classified information or other protected information described in paragraph (f) of this section.

(ii) Within 30 days after receiving the applicant's request for materials or written reply, TSA may request additional information or documents from the applicant that TSA believes are necessary to make a Final Determination.

(3) *Correction of records.* If the Initial Determination of Threat Assessment was based on a record that the applicant believes is erroneous, the applicant may correct the record, as follows:

(i) The applicant may contact the jurisdiction or entity responsible for the information and attempt to correct or complete information contained in his or her record.

(ii) The applicant must provide TSA with the revised record, or a certified true copy of the information from the

appropriate entity, before TSA may determine that the applicant meets the standards for the security threat assessment.

(4) *Reply.* (i) The applicant may serve upon TSA a written reply to the Initial Determination of Threat Assessment within 30 days after service of the Initial Determination, or 30 days after the date of service of TSA's response to the applicant's request for materials under paragraph (d)(2) of this section, if the applicant served such request. The reply must include the rationale and information on which the applicant disputes TSA's Initial Determination.

(ii) In an applicant's reply, TSA will consider only material that is relevant to whether the applicant meets the standards described in paragraph (d) of this section for the security threat assessment in paragraph (b) of this section.

(5) *Final determination.* Within 30 days after TSA receives the applicant's reply, TSA serves a Final Determination of Threat Assessment or a Withdrawal of the Initial Determination as provided in paragraphs (d) or (e) of this section.

(d) *Final Determination of Threat Assessment.* (1) In the case of an appeal of an Initial Determination of Threat Assessment that is based on criminal offense under §1572.103; immigration status under §1572.105; or mental competency under §1572.109; if the Director concludes that the applicant does not meet the security threat assessment standards described in §1572.5, TSA serves a Final Determination of Threat Assessment upon the applicant and the issuing State.

(2) In the case of an appeal of an Initial Determination of Threat Assessment that is based on a threat to national security or transportation security, or of terrorism under §1572.107, if the Assistant Secretary concludes that the applicant does not meet the security threat assessment standards described in §1572.5, TSA serves a Final Determination of Threat Assessment upon the applicant and issuing State.

(3) The Final Determination includes a statement that the Director or Assistant Secretary has reviewed the Initial Determination, the applicant's

§ 1572.143

49 CFR Ch. XII (10–1–05 Edition)

reply and any accompanying information, if any, and any other materials or information available to him or her and has determined that the applicant poses a security threat warranting denial of an HME.

(e) *Withdrawal of Initial Determination.* If the Director or Assistant Secretary concludes that the applicant does not pose a security threat warranting denial of the HME, TSA serves a Withdrawal of the Initial Determination upon the applicant.

(f) *Nondisclosure of certain information.* In connection with the procedures under this section, TSA does not disclose classified information to the applicant, as defined in Executive Order 12968 section 1.1(d), and reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

(g) *Extension of time.* TSA may grant an applicant an extension of time of the limits described in this section for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended. TSA may grant itself an extension of time for good cause.

(h) *Judicial review.* For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order in accordance with 49 U.S.C. 46110.

(i) *Appeal of immediate revocation.* (1) If TSA directs a State to revoke an HME pursuant to §1572.13(a) by issuing an Initial Determination of Threat Assessment and Immediate Revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (c) of this section.

§ 1572.143 Waiver procedures.

(a) *Scope.* This section applies to an applicant who—

(1) Has a disqualifying criminal offense described in §1572.103(a)(5) through (a)(9), and paragraph 1572.103(a)(10) if the underlying criminal offense is in paragraphs 1572.103(a)(5) through (a)(9); or

(2) Has a disqualifying criminal offense described in §1572.103(b); or

(3) Lacks mental capacity as described in §1572.109.

(b) *Waivers.* (1) An applicant initiates a waiver request by sending a written request to TSA for a waiver at any time, but not later than 30 days after the date of service of the Final Determination of Threat Assessment.

(2) In determining whether to grant a waiver, TSA will consider the following factors:

(i) The circumstances of the disqualifying act or offense;

(ii) Restitution made by the applicant;

(iii) Any Federal or State mitigation remedies;

(iv) Court records or official medical release documents indicating that the individual no longer lacks mental capacity;

(v) Other factors that indicate the applicant does not pose a security threat warranting denial of the HME.

(c) *Grant or denial of waivers.* The Director will send a written decision granting or denying the waiver to the applicant and a Determination of No Security Threat to the State in which the applicant applied for the HME, within 30 days after service the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(d) *Extension of time.* TSA may grant an applicant an extension of time of the limits described in paragraph (b) and (c) of this section for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended. TSA may grant itself an extension of time for good cause.

Subpart C—Transportation of Explosives From Foreign Locations

§ 1572.201 Transportation of explosives from Canada to the United States via commercial motor vehicle.

(a) *Applicability.* This section applies to carriers that carry explosives from Canada to the United States using a driver who is not a United States citizen or lawful permanent resident alien of the United States.

(b) *Terms used in this section.* For purposes of this section:

Carrier means any “motor carrier” or “motor private carrier” as defined in 49 U.S.C. 13102(12) and (13), respectively.

Customs Service means the United States Customs Service.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known driver means a driver of a motor vehicle who has been determined by the Governments of Canada and the United States to present no known security concern.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Lawful permanent resident alien means a lawful permanent resident alien of the United States as defined by 8 U.S.C. 1101(a)(2).

Offeror means the person offering a shipment to the carrier for transportation from Canada to the United States, and may also be known as the “consignor” in Canada.

(c) *Prior approval of carrier, offeror, and driver.* (1) No carrier may transport in commerce any explosive into the United States from Canada via motor vehicle if the driver of the vehicle is a not a United States citizen or lawful permanent resident alien unless the carrier, offeror, and driver are identified on a TSA list as a known carrier, known offeror, and known driver, respectively.

(2) The carrier must ensure that it, its offeror, and its driver have been determined to be a known carrier, known offeror, and known driver, respectively. If any has not been so determined, the carrier must submit the following information to Transport Canada:

(i) The carrier must provide its:

- (A) Official name;
- (B) Business number;
- (C) Any trade names; and
- (D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

- (A) Official name;
- (B) Business number; and
- (C) Address.

(iii) The following information about any driver the carrier may use to transport explosives into the United States from Canada who is neither a United States citizen nor lawful permanent resident alien of the United States:

- (A) Full name;
- (B) Canada Commercial Driver’s License number; and
- (C) Both current and most recent prior residential addresses.

(3) Transport Canada will determine that the carrier and offeror are legitimately doing business in Canada and will also determine that the drivers are properly licensed and present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known carriers, offerors, and drivers and their identifying information.

(4) TSA will update and maintain the list of known carriers, offerors, and drivers and forward the list to the Customs Service.

(5) Once included on the list, the carriers, offerors, and drivers need not obtain prior approval for future transport of explosives under this section.

(d) *TSA checks.* TSA may periodically check the data on the carriers, offerors and drivers to confirm their continued eligibility and may remove from the list any that TSA determines is not known or is a threat to security.

(e) *At the border—*

(1) *Driver who is not a United States citizen or lawful permanent resident alien.* Upon arrival at the border, and prior to entry into the United States, the driver must provide a valid Canadian commercial driver’s license to the Customs Service.

(2) *Driver who is a United States citizen or lawful permanent resident alien.* If the Customs Service cannot verify that the

driver is on the list, and if the driver is a United States citizen or lawful permanent resident alien, the driver may be cleared by the Customs Service upon providing:

- (i) A valid United States passport; or
- (ii) One or more other document(s) including a form of United States Federal or state government-issued identification with photograph, acceptable to the Customs Service.

(3) *Compliance.* If a carrier attempts to enter the United States without having complied with this section, the Customs Service will deny entry of the explosives and may take other appropriate action.

§ 1572.203 Transportation of explosives from Canada to the United States via railroad carrier.

(a) *Applicability.* This section applies to railroad carriers that carry explosives from Canada to the United States using a train crew member who is not a United States citizen or lawful permanent resident alien of the United States.

(b) *Terms under this section.* For purposes of this section:

Customs Service means the United States Customs Service.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known railroad carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known train crew member means an individual used to transport explosives from Canada to the United States who has been determined by the Govern-

ments of Canada and the United States to present no known security concern.

Lawful permanent resident alien means a lawful permanent resident alien of the United States as defined by 8 U.S.C. 1101(a)(2).

Offeror means the person offering a shipment to the railroad carrier for transportation from Canada to the United States, and may also be known as the “consignor” in Canada.

Railroad carrier means “railroad carrier” as defined in 49 U.S.C. 20102.

(c) *Prior approval of railroad carrier, offeror, and train crew member.* (1) No railroad carrier may transport in commerce any explosive into the United States from Canada via a train operated by a crew member who is not a United States citizen or lawful permanent resident alien unless the railroad carrier, offeror, and train crew member are identified on a TSA list as a known railroad carrier, known offeror, and known train crew member, respectively.

(2) The railroad carrier must ensure that it, its offeror, and each of its crew members have been determined to be a known railroad carrier, known offeror, and known train crew member, respectively. If any has not been so determined, the railroad carrier must submit the following information to Transport Canada:

(i) The railroad carrier must provide its:

- (A) Official name;
- (B) Business number;
- (C) Any trade names; and
- (D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

- (A) Official name;
- (B) Business number; and
- (C) Address.

(iii) The following information about any train crew member the railroad carrier may use to transport explosives into the United States from Canada who is neither a United States citizen nor lawful permanent resident alien:

- (A) Full name; and
- (B) Both current and most recent prior residential addresses.

(3) Transport Canada will determine that the railroad carrier and offeror

are legitimately doing business in Canada and will also determine that the train crew members present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known railroad carriers, offerors, and train crew members and their identifying information.

(4) TSA will update and maintain the list of known railroad carriers, offerors, and train crew members and forward the list to the Customs Service.

(5) Once included on the list, the railroad carriers, offerors, and train crew members need not obtain prior approval for future transport of explosives under this section.

(d) *TSA checks.* TSA may periodically check the data on the railroad carriers, offerors, and train crew members to confirm their continued eligibility and may remove from the list any that TSA determines is not known or is a threat to security.

(e) *At the border* (1) *Train crew members who are not United States citizens or lawful permanent resident aliens.* Upon arrival at a point designated by the Customs Service for inspection of trains crossing into the United States, the train crew members of a train transporting explosives must provide sufficient identification to the Customs Service to enable that agency to determine if each crew member is on the list of known train crew members maintained by TSA.

(2) *Train crew members who are United States citizens or lawful permanent resident aliens.* If the Customs Service cannot verify that the crew member is on the list and the crew member is a United States citizen or lawful permanent resident alien, the crew member may be cleared by the Customs Service upon providing:

(i) A valid United States passport; or
 (ii) One or more other document(s) including a form of United States Federal or state government-issued identification with photograph, acceptable to the Customs Service.

(3) *Compliance.* If a carrier attempts to enter the United States without having complied with this section, the Customs Service will deny entry of the

explosives and may take other appropriate action.

Subpart D—Fees for Security Threat Assessments for Individuals

SOURCE: 70 FR 2558, Jan. 13, 2005, unless otherwise noted.

§ 1572.301 Scope and definitions.

(a) *Scope.* This part applies to:

(1) States that issue a hazardous materials endorsement for a commercial driver's license;

(2) Individuals who apply for or renew a hazardous materials endorsement for a commercial driver's license and must undergo a security threat assessment under 49 CFR part 1572; and

(3) Entities who collect fees from such individuals on behalf of TSA.

(b) *Terms.* As used in this part:

Commercial driver's license (CDL) is used as defined in 49 CFR 383.5.

Day means calendar day.

Endorsement is used as defined in 49 CFR 383.5.

FBI Fee means the fee required for the cost of the Federal Bureau of Investigation to process fingerprint identification records and name checks.

Hazardous materials means any material that has been designated as hazardous under 49 U.S.C. 5103 and is required to be placarded under subpart F of 49 CFR part 172 or any quantity of a material listed as a select agent or toxin in 42 CFR part 73.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, which must be issued on the individual's commercial driver's license.

Information Collection Fee means the fee required in this part for the cost of collecting and transmitting fingerprints and other applicant information under 49 CFR part 1572.

State means a State of the United States or the District of Columbia.

Threat Assessment Fee means the fee required in this part for the cost of TSA adjudicating security threat assessments, appeals, and waivers under 49 CFR part 1572.

TSA agent means an entity approved by TSA to collect and transmit fingerprints and applicant information in accordance with 49 CFR part 1572 and fees in accordance with this part.

§§ 1572.303–1572.399 [Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

SOURCE: 70 FR 2558, Jan. 13, 2005, unless otherwise noted.

§ 1572.401 Fee collection options.

(a) *State collection and transmission.* If a State collects fingerprints and applicant information under 49 CFR part 1572, the State must collect and transmit to TSA the Threat Assessment Fee in accordance with the requirements of § 1572.403. The State also must collect and remit the FBI Fee in accordance with established procedures.

(b) *TSA agent collection and transmission.* If a TSA agent collects fingerprints and applicant information under 49 CFR part 1572, the agent must—

(1) Collect the Information Collection Fee, Threat Assessment Fee, and FBI Fee in accordance with procedures approved by TSA;

(2) Transmit to TSA the Threat Assessment Fee in accordance with procedures approved by TSA; and

(3) Transmit to TSA the FBI Fee in accordance with procedures approved by TSA and the Federal Bureau of Investigation.

§ 1572.403 Fee procedures for collection by States.

This section describes the procedures that a State that collects fingerprints and applicant information under 49 CFR part 1572, and the procedures an individual who applies for a new HME or renewal of an existing HME for a CDL in that State, must follow for collection and transmission of the Threat Assessment Fee and the FBI Fee.

(a) *Imposition of fees.* (1) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment under 49 CFR part 1572 for an individual who applies for a new HME or renewal of an existing HME: \$34.

(2) The following FBI Fee is required for the FBI to process fingerprint iden-

tification records and name checks required under 49 CFR part 1572: the fee collected by the FBI under 28 U.S.C. 534.

(3) An individual who applies for a new or renewed HME, or the individual's employer, must remit to the State the Threat Assessment Fee and the FBI Fee, in a form and manner approved by TSA and the State, when the individual submits the application for the HME to the State.

(b) *Collection of fees.* (1) A State must collect the Threat Assessment Fee and FBI Fee when an individual submits an application to the State for a new HME or renewal of an existing HME.

(2) Once TSA receives an application from a State for a security threat assessment under 49 CFR part 1572, the State is liable for the Threat Assessment Fee.

(3) Nothing in this subpart prevents a State from collecting any other fees that a State may impose on an individual who applies for a new HME or renewal of an existing HME.

(c) *Handling of fees.* (1) A State must safeguard all Threat Assessment Fees from the time of collection until remittance to TSA.

(2) All Threat Assessment Fees are held in trust by a State for the beneficial interest of the United States in paying for the costs of conducting the security threat assessment required by 49 U.S.C. 5103a and 49 CFR part 1572. A State holds neither legal nor equitable interest in the Threat Assessment Fees except for the right to retain any accrued interest on the principal amounts collected pursuant to this section.

(3) A State must account for Threat Assessment Fees separately, but may commingle such fees with other sources of revenue.

(d) *Remittance of fees.* (1) TSA will generate and provide an invoice to a State on a monthly basis. The invoice will indicate the total fee dollars (number of applicants times the Threat Assessment Fee) that are due for the month.

(2) A State must remit to TSA full payment for the invoice within 30 days after TSA sends the invoice.

(3) TSA accepts Threat Assessment Fees only from a State, not from an individual applicant for an HME.

(4) A State may retain any interest that accrues on the principal amounts collected between the date of collection and the date the Threat Assessment Fee is remitted to TSA in accordance with paragraph (d)(2) of this section.

(5) A State may not retain any portion of the Threat Assessment Fee to offset the costs of collecting, handling, or remitting Threat Assessment Fees.

(6) Threat Assessment Fees remitted to TSA by a State must be in U.S. currency and made payable to the "Transportation Security Administration."

(7) Threat Assessment Fees must be remitted by check, money order, wire or any other payment method acceptable to TSA.

(8) TSA will not issue any refunds of Threat Assessment Fees.

(9) If a State does not remit the Threat Assessment Fees for any month, TSA may decline to process any HME applications from that State.

§ 1572.405 Fee procedures for collection by TSA agents.

This section describes the procedures that an individual who applies for a new HME or renewal of an existing HME for a CDL must follow if a TSA agent collects and transmits the Information Collection Fee, Threat Assessment Fee, and FBI Fee.

(a) *Imposition of fees.* (1) The following Information Collection Fee is required for a TSA agent to collect and transmit fingerprints and applicant infor-

mation in accordance with 49 CFR part 1572: \$38.

(2) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment under 49 CFR part 1572 for an individual who applies for a new HME or renewal of an existing HME: \$34.

(3) The following FBI Fee is required for the FBI to process fingerprint identification records and name checks required under 49 CFR part 1572: The fee collected by the FBI under 28 U.S.C. 534.

(4) An individual who applies for a new or renewed HME, or the individual's employer, must remit to the TSA agent the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in a form and manner approved by TSA, when the individual submits the application required under 49 CFR part 1572.

(b) *Collection of fees.* A TSA agent will collect the fees required under this section when an individual submits an application to the TSA agent in accordance with 49 CFR part 1572.

(c) *Remittance of fees.* (1) Fees required under this section that are remitted to a TSA agent must be made in U.S. currency and made payable to the "Transportation Security Administration."

(2) Fees required under this section must be remitted by check, money order, wire or any other payment method acceptable to TSA.

(3) TSA will not issue any refunds of fees required under this section.

(4) Applications submitted in accordance with 49 CFR part 1572 will be processed only upon receipt of all applicable fees under this section.



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.

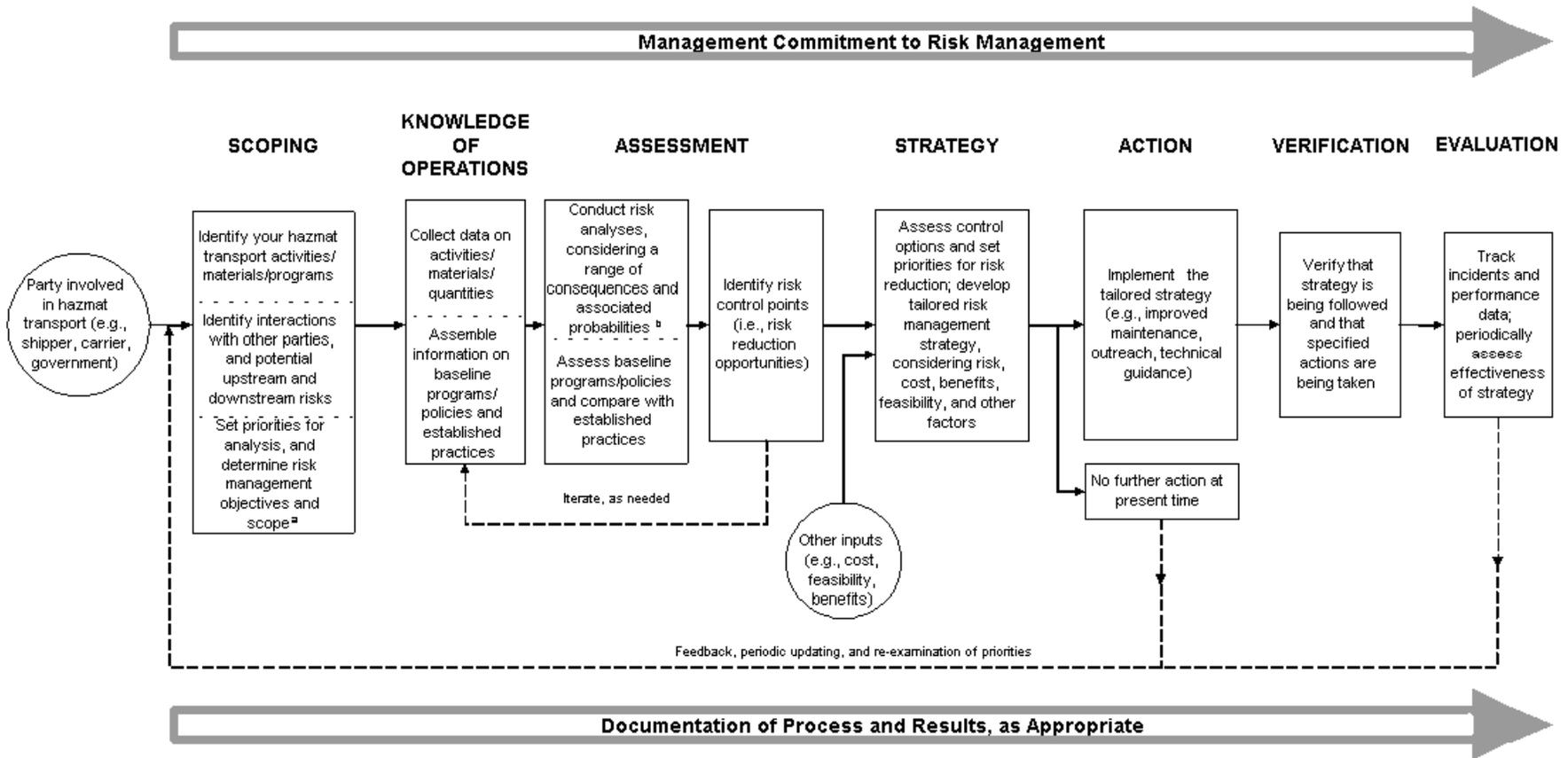
These steps of the RMSEF (see flowchart exhibit) are sufficiently general that the framework can be customized to address a variety of risk management issues and achieve measurable improvements. It is adaptable by shippers and carriers to systematically help in securing their hazardous materials shipments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

§ 11.121

the importance of the knowledge gained or to be gained.

(b) On the basis of this evaluation, the department or agency head may approve or disapprove the application or proposal, or enter into negotiations to develop an approvable one.

§ 11.121 [Reserved]

§ 11.122 Use of Federal funds.

Federal funds administered by a department or agency may not be expended for research involving human subjects unless the requirements of this policy have been satisfied.

§ 11.123 Early termination of research support: Evaluation of applications and proposals.

(a) The department or agency head may require that department or agency support for any project be terminated or suspended in the manner prescribed in applicable program requirements, when the department or agency head finds an institution has materially failed to comply with the terms of this policy.

(b) In making decisions about supporting or approving applications or proposals covered by this policy the department or agency head may take into account, in addition to all other eligibility requirements and program criteria, factors such as whether the applicant has been subject to a termination or suspension under paragraph (a) of this section and whether the applicant or the person or persons who would direct or has/have directed the scientific and technical aspects of an activity has/have, in the judgment of the department or agency head, materially failed to discharge responsibility for the protection of the rights and welfare of human subjects (whether or not the research was subject to Federal regulation).

§ 11.124 Conditions.

With respect to any research project or any class of research projects the department or agency head may impose additional conditions prior to or at the time of approval when in the judgment of the department or agency head additional conditions are necessary for the protection of human subjects.

49 CFR Subtitle A (10–1–06 Edition)

PART 15—PROTECTION OF SENSITIVE SECURITY INFORMATION

Sec.

- 15.1 Scope.
- 15.3 Terms used in this part.
- 15.5 Sensitive security information.
- 15.7 Covered persons.
- 15.9 Restrictions on the disclosure of SSI.
- 15.11 Persons with a need to know.
- 15.13 Marking SSI.
- 15.15 SSI disclosed by DOT.
- 15.17 Consequences of unauthorized disclosure of SSI.
- 15.19 Destruction of SSI.

AUTHORITY: 49 U.S.C. 40119.

SOURCE: 69 FR 28078, May 18, 2004, unless otherwise noted.

§ 15.1 Scope.

(a) *Applicability.* This part governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information, as defined in §15.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

(b) *Delegation.* The authority of the Secretary under this part may be further delegated within DOT.

§ 15.3 Terms used in this part.

In addition to the terms in §15.3 of this chapter, the following terms apply in this part:

Administrator means the Under Secretary of Transportation for Security referred to in 49 U.S.C. 114(b), or his or her designee.

Coast Guard means the United States Coast Guard.

Covered person means any organization, entity, individual, or other person

described in §15.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in §15.7.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.

Federal Flight Deck Officer means a pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations.

Maritime facility means any facility as defined in 33 CFR part 101.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term *record* also includes any draft, proposed, or recommended change to any record.

Security contingency plan means a plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security program means a program or plan and any amendments developed for the security of the following, including any comments, instructions, or implementing guidance:

- (1) An airport, aircraft, or aviation cargo operation;
- (2) A maritime facility, vessel, or port area; or

- (3) A transportation-related automated system or network for information processing, control, and communications.

Security screening means evaluating a person or property to determine whether either poses a threat to security.

SSI means sensitive security information, as described in §15.5.

Threat image projection system means an evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment.

TSA means the Transportation Security Administration.

Vulnerability assessment means any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A *vulnerability assessment* may include proposed, recommended, or directed actions or countermeasures to address security concerns.

§15.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 40119(b)(1), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which the Secretary of DOT has determined would—

- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

- (2) Reveal trade secrets or privileged or confidential information obtained from any person; or

- (3) Be detrimental to transportation safety.

(b) *Information constituting SSI.* Except as otherwise provided in writing by the Secretary of DOT in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

§ 15.5

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including—

(i) Any aircraft operator or airport operator security program or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information Circular issued by TSA under 49 CFR 1542.303 or 1544.305, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

49 CFR Subtitle A (10–1–06 Edition)

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(9) *Security screening information.* The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.* (i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport or a secure or

restricted area of a maritime facility, port area, or vessel or;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.*

(i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying

§ 15.7

out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* The Secretary of DOT may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

§ 15.7 Covered persons.

Persons subject to the requirements of part 15 are:

(a) Each airport operator and aircraft operator subject to the requirements of Subchapter C of this title.

(b) Each indirect air carrier, as defined in 49 CFR 1540.5.

(c) Each owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators, required to have a security plan under Federal or International law.

(d) Each owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub. L. 107-295), 46 U.S.C. 70101 *et seq.*, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.*

(e) Each person performing the function of a computer reservation system or global distribution system for airline passenger information.

49 CFR Subtitle A (10-1-06 Edition)

(f) Each person participating in a national or area security committee established under 46 U.S.C. 70112, or a port security committee.

(g) Each industry trade association that represents covered persons and has entered into a non-disclosure agreement with the DHS or DOT.

(h) DHS and DOT.

(i) Each person conducting research and development activities that relate to aviation or maritime transportation security and are approved, accepted, funded, recommended, or directed by DHS or DOT.

(j) Each person who has access to SSI, as specified in §15.11.

(k) Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

(l) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DOT, DHS, or that has prepared a vulnerability assessment that will be provided to DOT or DHS in support of a Federal security program.

(m) Each person receiving SSI under §1520.15(d) or (e).

§ 15.9 Restrictions on the disclosure of SSI.

(a) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in §15.13.

(5) Dispose of SSI as specified in §15.19.

(b) *Unmarked SSI.* If a covered person receives a record containing SSI that is not marked as specified in §1520.13, the covered person must—

(1) Mark the record as specified in § 15.13; and

(2) Inform the sender of the record that the record must be marked as specified in § 15.13.

(c) *Duty to report unauthorized disclosure.* When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional requirements for critical infrastructure information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

§ 15.11 Persons with a need to know.

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) *Federal employees, contractors, and grantees.* (1) A Federal employee has a need to know SSI if access to the infor-

mation is necessary for performance of the employee's official duties.

(2) A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) *Background check.* The Secretary of DOT may make an individual's access to the SSI contingent upon satisfactory completion of a security background check and the imposition of procedures and requirements for safeguarding SSI that are satisfactory to the Secretary.

(d) *Need to know further limited by the DHS or DOT.* For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

[69 FR 28078, May 18, 2004, as amended at 70 FR 1381, Jan. 7, 2005]

§ 15.13 Marking SSI.

(a) *Marking of paper records.* In the case of paper records containing SSI, a covered person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom, of—

(1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;

(2) Any title page; and

(3) Each page of the document.

(b) *Protective marking.* The protective marking is: SENSITIVE SECURITY INFORMATION.

(c) *Distribution limitation statement.* The distribution limitation statement is:

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.

(d) *Other types of records.* In the case of non-paper records that contain SSI,

§ 15.15

including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

§ 15.15 SSI disclosed by DOT.

(a) *In general.* Except as otherwise provided in this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does DOT release such records to persons without a need to know.

(b) *Disclosure under the Freedom of Information Act and the Privacy Act.* If a record contains both SSI and information that is not SSI, DOT, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) *Disclosures to committees of Congress and the General Accounting Office.* Nothing in this part precludes DOT from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) *Disclosure in enforcement proceedings—(1) In general.* The Secretary of DOT may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the Secretary, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by DOT.

(2) *Security background check.* Prior to providing SSI to a person under paragraph (d)(1) of this section, the Secretary of DOT may require the individual or, in the case of an entity, the individuals representing the entity, and their counsel, to undergo and satisfy, in the judgment of the Secretary of DOT, a security background check.

49 CFR Subtitle A (10–1–06 Edition)

(e) *Other conditional disclosure.* The Secretary of DOT may authorize a conditional disclosure of specific records or information that constitute SSI upon the written determination by the Secretary that disclosure of such records or information, subject to such limitations and restrictions as the Secretary may prescribe, would not be detrimental to transportation safety.

(f) *Obligation to protect information.* When an individual receives SSI pursuant to paragraph (d) or (e) of this section that individual becomes a covered person under § 15.7 and is subject to the obligations of a covered person under this part.

(g) *No release under FOIA.* When DOT discloses SSI pursuant to paragraphs (b) through (e) of this section, DOT makes the disclosure for the sole purpose described in that paragraph. Such disclosure is not a public release of information under the Freedom of Information Act.

(h) *Disclosure of Critical Infrastructure Information.* Disclosure of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act is governed solely by the requirements of section 214 and any implementing regulations.

§ 15.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DOT, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

§ 15.19 Destruction of SSI.

(a) *DOT.* Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DOT destroys SSI when no longer needed to carry out the agency's function.

(b) *Other covered persons—(1) In general.* A covered person must destroy SSI completely to preclude recognition or reconstruction of the information

when the covered person no longer needs the SSI to carry out transportation security measures.

(2) *Exception.* Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under State or local law.

PART 17—INTERGOVERNMENTAL REVIEW OF DEPARTMENT OF TRANSPORTATION PROGRAMS AND ACTIVITIES

Sec.

- 17.1 What is the purpose of these regulations?
- 17.2 What definitions apply to these regulations?
- 17.3 What programs and activities of the Department are subject to these regulations?
- 17.4 [Reserved]
- 17.5 What is the Secretary's obligation with respect to Federal interagency coordination?
- 17.6 What procedures apply to the selection of programs and activities under these regulations?
- 17.7 How does the Secretary communicate with state and local officials concerning the Department's programs and activities?
- 17.8 How does the secretary provide states an opportunity to comment on proposed Federal financial assistance and direct Federal development?
- 17.9 How does the Secretary receive and respond to comments?
- 17.10 How does the Secretary make efforts to accommodate intergovernmental concerns?
- 17.11 What are the Secretary's obligations in interstate situations?
- 17.12 How may a state simplify, consolidate, or substitute federally required state plans?
- 17.13 May the Secretary waive any provision of these regulations?

AUTHORITY: Executive Order 12372, July 14, 1982 (47 FR 30959), as amended April 8, 1983 (48 FR 15887); sec. 401 of the Intergovernmental Cooperation Act of 1968, as amended (31 U.S.C. 6506); sec. 204 of the Demonstration Cities and Metropolitan Development Act of 1966, as amended (42 U.S.C. 3334).

SOURCE: 48 FR 29272, June 24, 1983, unless otherwise noted.

§ 17.1 What is the purpose of these regulations?

(a) The regulations in this part implement Executive Order 12372, "Inter-

governmental Review of Federal Programs," issued July 14, 1982, and amended on April 8, 1983. These regulations also implement applicable provisions of section 401 of the Intergovernmental Cooperation Act of 1968 and section 204 of the Demonstration Cities and Metropolitan Development Act of 1966.

(b) These regulations are intended to foster an intergovernmental partnership and a strengthened Federalism by relying on state processes and on state, areawide, regional and local coordination for review of proposed Federal financial assistance and direct Federal development.

(c) These regulations are intended to aid the internal management of the Department, and are not intended to create any right or benefit enforceable at law by a party against the Department or its officers.

§ 17.2 What definitions apply to these regulations?

Department means the U.S. Department of Transportation.

Order means Executive Order 12372, issued July 14, 1982, and amended April 8, 1983, and titled "Intergovernmental Review of Federal Programs."

Secretary means the Secretary of the U.S. Department of Transportation or an official or employee of the Department acting for the Secretary under a delegation of authority.

State means any of the 50 states, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, Guam, American Samoa, the U.S. Virgin Islands, or the Trust Territory of the Pacific Islands.

§ 17.3 What programs and activities of the Department are subject to these regulations?

The Secretary publishes in the FEDERAL REGISTER a list of the Department's programs and activities that are subject to these regulations and identifies which of these are subject to the requirements of section 204 of the Demonstration Cities and Metropolitan Development Act.

GUIDE TO DEVELOPING AN EFFECTIVE SECURITY PLAN FOR THE HIGHWAY TRANSPORTATION OF HAZARDOUS MATERIALS

Developed by

Battelle and TotalSecurity.US

for

Federal Motor Carrier Safety Administration

U.S. Department of Transportation

Washington, DC 20590



TABLE OF CONTENTS

Executive Summary.....	iii
Introduction	1
How to Use This Document	3
Chapter One: Security Assessment	5
Part A. Reviewing Your Hazmat Operations.....	5
Part B. Identifying Relevant Threats and Vulnerabilities.....	6
Part C. Addressing the Transportation of Specific Hazardous Materials.....	7
Part D. Addressing Your Specific Operations.....	8
Part E. Prioritizing Threats and Vulnerabilities.....	9
Chapter Two: Security Plan	11
Part A. Primary Security Objectives.....	12
Part B. Specific Security Measures.....	12
Part C. Addressing Varying Threat Levels	14
Part D. Security Plan Components.....	16
Part E. Example.....	17
Part F. Corporate vs. Terminal Level Planning.....	18
Chapter Three: Security Training.....	19
Part A. Security Awareness Training.....	19
Part B. In-Depth Security Training.....	19
Part C. Recurrent Training and Recordkeeping.....	20
Chapter Four: Security Plan Administration.....	21
Part A. Distribution and Availability.....	21
Part B. Updates and Maintenance.....	21
Part C. Verification and Evaluation.....	22
Part D. Coordination, Cooperation, and Liaisons	22
Appendix A: Understanding the Security Threat.....	23
Appendix B: Issues to Consider in Your Security Assessment.....	27
Appendix C: Sample Security Plan Measures.....	33
Appendix D: FMCSA Security Contact Reviews.....	41
Appendix E: References.....	47
Appendix F: Helpful Industry Web Sites	48

EXECUTIVE SUMMARY

This Guide is a tool that motor carriers transporting hazardous materials can use in developing a security plan as required by the U.S. Department of Transportation in their HM-232 rulemaking [1]. It is designed to provide motor carriers with (a) sufficient background to understand the nature of the threats against hazardous materials transportation; (b) the means to identify the vulnerabilities to those threats; and (c) an approach to address the vulnerabilities.

The first step in developing a security plan is conducting a security assessment. The Guide establishes a framework for reviewing a company's hazardous materials operations and identifying relevant threats and vulnerabilities. The focus is on making the assessment specific with respect to an individual company facility or each type of hazardous material. The Guide also offers an approach for prioritizing each of the threats and vulnerabilities that are identified.

The discussion of the security plan introduces a recommended approach for determining appropriate security measures for addressing identified threats and vulnerabilities that help to eliminate unnecessary security-related expenses. Consideration of varying threat levels (such as those indicated by the Homeland Security Advisory System) and a method for prioritizing potential security measures is also discussed.

The Guide covers the required security training (awareness and in-depth) and security plan administration. Administration includes the distribution, maintenance, verification, and validation of the full security plan as well as how to best incorporate the insights and support that are available from industry partners, local community organizations, and law enforcement agencies.

INTRODUCTION

Hazardous materials in transportation are vulnerable to sabotage or misuse and in the wrong hands pose a significant security threat. The security of hazardous materials in transportation poses unique challenges as compared to security at fixed facilities because of the changing environment surrounding a moving vehicle. Since hazardous materials are frequently transported in large quantities, once mobile they are particularly vulnerable to theft, interception, detonation, or release. When transported in proximity to large population centers, accidental or intentional acts could have serious consequences.

Due to the terrorist attacks committed on September 11, 2001, and subsequent threats to the transportation system, the Federal Motor Carrier Safety Administration (FMCSA) conducted over 30,000 Security Sensitivity Visits (SSVs) between October 2001 and April 2002. The SSVs consisted of face-to-face meetings between FMCSA or state investigators and top carrier officials to assess security vulnerabilities and identify countermeasures that can improve security. FMCSA then began including SSVs as part of all compliance reviews on hazardous materials (HM) carriers to encourage a high level of vigilance within the industry.

Also prompted by the September 11, 2001, terrorist attacks and subsequent threats related to biological and other types of hazardous materials, the Department of Transportation's Research and Special Programs Administration (RSPA) issued new regulations under Docket No. HM-232 intended to enhance the security of hazardous materials transportation [1]. As discussed in more detail below, the new regulations impose security plan and security training requirements on certain hazardous materials shippers and carriers.

The Research and Special Programs Administration, which has regulatory authority over hazardous materials transportation across all modes, published the HM-232 final rule on March 25, 2003. The HM-232 regulations require persons who offer certain types and quantities of hazardous materials (hazmat) for transportation or transport in commerce to develop and implement security plans by September 25, 2003. In addition, all hazmat employees, as defined in the Hazardous Materials Regulations (HMR, 49 CFR Parts 171-180), must receive training that provides an awareness of security risks associated with hazmat transportation and methods designed to enhance hazmat transportation security.

Persons who offer for transportation or transport the following hazardous materials must develop and implement security plans that conform to the HM-232 requirements:

HAZARDOUS MATERIALS SHIPMENTS SUBJECT TO HM-232	
Material	Threshold (if specified)
Class 7 – Radioactive	Highway route controlled quantity (HRCQ)
Division 1.1, 1.2, or 1.3 – Explosive	More than 25 kg (55 pounds)
PIH in Hazard Zone A	More than 1 liter (1.06 quarts) (container)
HM in a bulk packaging (container)	Capacity of packaging equal to or greater than: Liquid or gas: 13,248 liters (3,500 gallons) Solid: 13.24 cubic meters (468 cubic feet)
HM in a non-bulk packaging	Total gross weight equal to or greater than 2,268 kg (5,000 pounds)
Select agent or toxin regulated by the Centers for Disease Control and Prevention (CDC)	
Any HM shipment requiring placarding according to subpart F of the HMR	

Many motor carriers include security measures in their standard operating policies and procedures. The HM-232 final rule requires a more systematic approach to transportation security and a specific focus on potential terrorist or criminal threats. While any plan that meets the specific provisions of the rule will be acceptable, many organizations will have to make adjustments to existing plans to cover all required areas. Other organizations will develop their security plans for the first time in response to this new regulation. The information in this Guide should serve as a tool in developing a security plan required by the U.S. Department of Transportation.

You should also be aware that the U.S. Patriot Act, passed in October 2001, included a provision for requiring background checks for individuals operating motor vehicles transporting hazardous materials [2]. The Transportation Security Administration (TSA) enacted regulations on May 5, 2003 implementing this provision. TSA's rule requires routine background checks for drivers with a hazmat endorsement on their Commercial Drivers License (CDL). The required background checks must include a review of criminal, immigration, and FBI records [3].

HOW TO USE THIS DOCUMENT

Although this Guide is directed at motor carriers that transport hazardous materials, hazmat shippers may also find this publication a useful tool. The information herein is a tool that you may apply in developing a security plan required by the U.S. Department of Transportation. While the main chapters guide you through the steps a motor carrier needs to take and the issues they need to consider, the appendices provide more in-depth information that will be helpful in the development of an effective security plan. Following is a review of the chapters and appendices:

- The Introduction provides a review of the security planning process and of the background for this Guide. If you would like more information about terrorists and their operations, refer to Appendix A.
- Chapter One guides you through your security assessment to identify the threats and vulnerabilities to your operations. A security assessment is a necessary first step in preparing your security plan. If you would like more detailed information on issues to consider, refer to Appendix B.
- Chapter Two addresses the detailed components that need to be included in your security plan and provides examples on how to construct the plan. Personnel security, unauthorized access, and en route security are specifically addressed. Additional guidance for companies with operations at many locations is also included. This chapter does NOT provide a comprehensive list of security measures for you to implement; rather, it guides you in determining which ones are right for you. Some examples are included in this chapter to get you started and more are included in Appendix C.
- Chapter Three discusses the required components of a training program and how to develop one.
- Chapter Four covers the administration of your security plan including how it is provided to your employees and maintained. This section also covers establishing relationships with other entities, such as local law enforcement, to augment and enhance your security.
- Appendix D outlines the approach that the Federal Motor Carrier Safety Administration (FMCSA) is taking to ensure that the highway transportation of hazardous materials is secure and that motor carriers are in regulatory compliance.
- Appendix E at the end of this Guide contains a list of references and citations.

ACRONYMS

CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CDL	Commercial Drivers License
DOT	U.S. Department of Transportation
DHS	U.S. Department of Homeland Security
FMCSA	Federal Motor Carrier Safety Administration (in DOT)
FBI	Federal Bureau of Investigation
HM-232	Security Requirements for Offerors and Transporters of Hazardous Materials, a rulemaking issued by RSPA
HM, hazmat	Hazardous Materials
HMR	Hazardous Materials Regulations
HRCQ	Highway Route-Controlled Quantity (of RAM)
HSAS	Homeland Security Advisory System (with five color-coded levels)
PIH	Poisonous by Inhalation (synonymous with Toxic by Inhalation)
PSO	Primary Security Objective
RAM	Radioactive Material
RSPA	Research and Special Programs Administration (in DOT)
SSV	Security Sensitivity Visit
TSA	Transportation Security Administration (in DHS)
WMD	Weapons of Mass Destruction

GLOSSARY

carrier	The company transporting a shipment from the shipper to the consignee
consignee	The company (or person) to which a shipment is destined (the receiver)
likelihood	The probability of something happening; for HM security, the <i>attractiveness</i> of something to a terrorist is used in place of likelihood.
may	Indicates an option for consideration only.
must	Indicates something which is <i>required</i> for you to do by regulation
non-specific but credible	Refers to a threat that is general in nature but is still believed to be realistic
primary security objective	Term used to represent a main goal in addressing security vulnerabilities; security measures are chosen to meet the primary objective
risk	Represents the exposure to a hazard; for HM security, risk is the likelihood of a terrorist act combined with its probable consequences
specific and credible	Refers to a threat that is focused (perhaps to a city, bridge, or industry) and believed to be realistic
specific security measure	A policy, procedure, device, etc. that is put in place to reduce one or more vulnerabilities that an organization may face
shipper	The offeror of the shipment for transportation (the origin)
should	Implies a <i>recommendation</i> only – it is not required
threat	A source of danger; for HM security, this includes terrorists and criminals and the types of attacks they might initiate to achieve their objectives
vulnerability	A weakness; susceptibility to attack or injury

CHAPTER ONE: SECURITY ASSESSMENT

One of the most critical components of HM-232 is the assessment of possible transportation security risks for covered shipments of hazardous materials. Many companies have implemented numerous security measures without examining the threats against their operations and their vulnerabilities to those threats. *Threats* are sources of danger and can include both criminals and terrorists and the attacks that they might initiate to achieve their objectives. *Vulnerabilities* are weaknesses that make you more susceptible to attack or injury.

HM-232 requires companies to complete a written security assessment and to develop a security plan that is based on the assessment. This Guide will assist motor carriers in conducting their security assessments and in developing their security plans.

Part A. Reviewing Your Hazmat Operations

When conducting a proper assessment of the threats to and vulnerabilities of your operation to a terrorist attack or terrorist activity, the types of information to consider include: (a) the type of hazardous material you transport, (b) the frequency and quantity of shipments, (c) the packaging type, and (d) the amount stored on-site. You will also need to identify and address your business practices (including relationships with external partners), such as the emergency response information that is available on site, and physical assets that are a part of your hazmat transportation activities.

A.1 Business Practices

You should analyze your company's business practices that affect the transportation of the hazardous materials included in HM-232 to identify potential security vulnerabilities. Such business practices may include:

- Taking and processing orders, including dispatching;
- Hiring and human resources-related activities (which relate to ensuring the trustworthiness of employees);
- Job descriptions, organization charts, and reporting structures for responsible management and decision making, security policies, and reporting (which all relate to who has access to information and who makes key decisions);
- Facility and building access policies and procedures;
- Qualification and selection of outside service providers (contractors) with access to hazmat handling areas; and
- Policies and procedures on distributing information related to hazmat shipments, including to business partners.

A.2 Physical Assets

You should analyze each physical asset (facility, terminal, etc.) used in the transportation of hazmat to identify potential security vulnerabilities. This analysis should consider, at a minimum, the following:

- Exterior surveillance and line-of-sight attack potential;
- Areas of concealment;
- Normal and potential vehicle and pedestrian paths;
- How congestion, choke points (where vehicles or pedestrians may get delayed during an evacuation), and other circumstances might reduce the effectiveness of your security measures;
- Your immediate surroundings – assess the potential for layered protection or and the nature of potential nearby threats;
- Storage facilities, transfer, loading, and unloading areas;
- Business offices, storage of empty hazmat packagings; and
- Visitor, vendor, and employee parking.

In addition, you should examine each configuration of transport vehicles for vulnerabilities based on use and the likely routes. Unlike many facilities, where the areas that are most in need of protection (such as critical operation centers) are separated from an outer fence by a considerable distance, there is no protective buffer surrounding vehicles on the road. Vehicles, therefore, can be more vulnerable. You should also identify and assess facilities that are owned and/or operated by others, such as truck stops, and rest/parking areas.

Part B. Identifying Relevant Threats and Vulnerabilities

It is important to remember that in the case of hazardous materials, the assumed agenda of terrorists is to convert the material, package, or vehicle into a weapon; in other words, controlling the material is an operational act in support of a larger attack plan. This can occur in several ways. The three principal methods are:

- The material can be purchased and delivered to the target location or an intermediate site to be transported later.
- The material can be acquired by theft either in transit or at a storage site. This part of the operation can take the forms of fraud, stealth, or violence.
- The material can be converted to weapons use directly while under legitimate control. This could be a violent event that takes the form of a catastrophic release, typically by explosive or mechanical attack.

Taking the case of the legitimate purchase, there is nothing in the HM-232 security requirements that calls for validation of the consignee. However, it would be prudent business practice (but not required) to verify that an order of unusual character, such as a large shipment of toxic-by-inhalation gas to a stadium, is in fact expected and required. When it comes to determining which security measures are appropriate for your company, such as checking with consignees, only you can be the judge.

Material acquired by theft is not unlike criminal activity associated with high value shipments. Unlike typical criminal profiles, however, the terrorist's readiness to employ extreme violence is much greater. Where the criminal may be reluctant to employ deadly force because of the repercussions if captured, the terrorist may not expect to survive the operation and so eventual capture is meaningless as a deterrent. Without considering the tactics used, a terrorist's objective is to take control of the material and transport it to a target location for use as a weapon. Maintaining control of the cargo, not the vehicle, is the primary concern here.

In the third case, the material is converted to a weapon on the spot. This means that the material must be located at or near the final target. Storage areas and transport routing that are near desirable targets should be areas of concern. The "Trojan Horse" scenario, where a device is attached to a shipment and detonated at the desired moment and location, and the "Intercept" where a device is located in anticipation of the material's passage, are the two most likely options.

What you can derive from all of the preceding discussion is that each method requires specific knowledge in order to be successful. There are basically three ways in which a terrorist can obtain this information:

- Conduct research of public records and reference materials, including company websites, annual reports, and marketing information;
- Observe operations; and
- Acquire knowledge from participants in the company's operations or by actually taking part themselves (as an "insider").

Public information may be of limited value beyond learning the characteristics of the material being pursued. Observation is an operational act that involves exposure and risk of discovery. Direct knowledge through participation or trust of those in a position to know provides both detail and a high level of confidence in the information. This is the reason why business processes are of a security concern to HM-232. For additional insight into terrorists and their operations, see Appendix A.

Part C. Addressing the Transportation of Specific Hazardous Materials

Although a major portion of the security plan may be uniform across a company's entire operation, planning must recognize that different classes of material may require different strategies. This is due to the nature of the material and the character of the transportation processes involved. The following is a discussion of several materials:

- Radioactive materials (RAM) are not likely to be used in creating a fission or fusion bomb, but as a persistent contaminant, that represents both a real health hazard and an emotional trigger for widespread panic. The most publicly discussed tactic is the "Dirty Bomb," more appropriately referred to as a "Radiological Dispersion Device" or RDD. This device uses conventional explosives to disperse the contamination, potentially creating an acute situation for large numbers of people. Because certain types of RAM are effectively invisible and easily spread through contact, less spectacular methods of dispersal must also be considered.

- Explosives require proximity to the target and sufficient quantity to be effective. By controlling either of these two parameters, the potential consequences can be reduced.
- Poisons are similar to RAM in that they represent a dispersal attack in order to be effective. Unlike RAM, dispersal of poisons must maintain an effective level of concentration to be successful. This tends to limit use of these materials to situations where the dispersal can occur within a defined volume.
- Flammables represent the most common category of hazardous material shipped and transported. The sheer number of opportunities and the diversity of locations and circumstances involved make flammable materials cause for concern.
- Biological materials represent means for dispersal attack, similar to RAM. CDC-regulated materials represent a potential for the introduction of infectious disease into the population.

Another category of hazardous materials of interest to HM-232 includes all other placarded materials. Although these may not present the level of weapons potential as those discussed above, some of them are capable of significant economic and social disruption when intentionally released with malicious intent, while others do not require any additional security measures to be implemented.

Part D. Addressing Your Specific Operations

Companies have different and distinct types of operations. For example, some companies act as both shipper and carrier. In addition, some carriers maintain their over-the-road operations entirely separate (and differently) from their local pick-up and delivery operations. It is appropriate to consider the distinct character of each of your operations in your security assessment.

HM-232 addresses the transportation of hazardous materials. It does not cover fixed facility operations unless those operations are incidental to transportation, such as loading, unloading, and certain temporary storage. At a shipper facility, the elements that you should examine include the preparation of hazmat for transportation, selection and use of appropriate packaging, preparation of shipping documentation, loading operations, and so on. To the extent that this information can be hidden, the vulnerability can be reduced. You may want to include issues related to long-term storage of hazmat at your facilities in your security assessment, but are not required to do so by HM-232.

Both shipper and carrier operations involve the processing of orders. The “business side of the house” is important because of the storage and shipping information. There are two groups of people of concern: those that must process or act on the order information and those who may have access to the information but do not typically process or act on it. Although each person who processes an order should be considered a potential threat, they also represent an opportunity for threat recognition.

Carrier operations present several difficult security issues. Effective status and tracking of the cargo may be impractical, forcing strategies that involve the personnel and transportation equipment as surrogate indicators to potential problems.

The variety of situations typically encountered while en route present many vulnerabilities that a terrorist can exploit.

Part E. Prioritizing Threats and Vulnerabilities

Companies have limited security dollars, making it necessary to prioritize the vulnerabilities to be addressed and the primary security objectives (PSOs).

There are many ways to do a prioritization, but most rely on some form of subjective ranking system. For example, you may prioritize the threats you face as highly likely, somewhat likely, possible, unlikely, or improbable (of course, you could use a greater or fewer number of categories). You may then rate your vulnerabilities (perhaps on a scale from very low to high), considering how easy you believe it would be to exploit that vulnerability given your current operations. Combining these categories can help you focus your energies and limited resources on those vulnerabilities most easily exploited that correspond to the highest threats. You can treat this combination of threats and vulnerabilities as the relative *likelihood* of a terrorist act. However, this is not likelihood in the traditional sense of the word, since there are not sufficient historical data to know the *probabilities* of any future terrorist acts; it is simply a good substitute. This analysis will help you see what terrorists find attractive. The table below shows one example—assigning a value from 1 to 4 to each combination of threat and vulnerability, with a value of 4 having the highest likelihood. Let’s say you have identified three threats to which you have some vulnerability. For one of these threats you have a single vulnerability that could be exploited; however, for the other two, you have two vulnerabilities each. This makes a total of five threat-vulnerability combinations. To prioritize these, you would place each of the five combinations in the appropriate cell in the table below.

"LIKELIHOOD"				
THREATS	VULNERABILITIES			
	Very Low	Low	Medium	High
Specific and Credible	2	3	4	4
Non-specific but Credible	2	3	3	4
Possible	1	2	3	3
Unlikely	1	2	2	2
Improbable	1	1	2	2

You may also wish to consider the potential consequences of a terrorist act in each case. For example, you may identify similar threats and vulnerabilities for operations involving different materials, but the consequences of one material may be worse than for the others. You could use a ranking scheme similar to the one used above in which you assign potential consequences to severe, high, medium, or low categories. Combining consequences with their “likelihoods” provides you with a measure of *risk*. Since our “likelihoods” are only approximations of the true probability of a terrorist event, the risk would also be a crude approximation of the actual risk. One way of combining likelihood and consequence to determine risk follows the same approach used above. Take each of the threat-vulnerability combinations (which represent the “likelihood”) and place them in the appropriate cell in the following table, depending on how severe the consequences would be if the threat were able to exploit that particular vulnerability.

“RISK”				
LIKELIHOOD	CONSEQUENCES			
	Low	Medium	High	Severe
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	2	2

Of course, you may choose to assign different values to the cells in these tables, but you should focus first on the elements in the top right of the “Risk” table. Anything you place in a cell with a value of 3 or 4, for example, might warrant further attention. Ultimately, you have to decide which vulnerabilities you need to address, but this approach provides you with a method for prioritizing them.

CHAPTER TWO: SECURITY PLAN

Your Security Plan should be a complete document and should include: (a) information on your security assessment; (b) how you address any vulnerabilities identified in the assessment; (c) what security measures you have adopted; (d) how, when, and by whom they will be implemented; (e) your organizational structure; and (f) the responsibilities of the various employee positions. In essence, your security plan is the detailed map of how you address the security assessment.

Each motor carrier should evaluate the threats it faces and its vulnerabilities based on its unique operations and facilities and should recognize that a cookie-cutter approach is not appropriate. The measures adopted by your company to address your vulnerabilities do not need to be complex or expensive to be effective, but the justification and rationale to support them needs to be sound and documented. The key to developing adequate security measures is to think “prevention.” Understand that the threat is very real and try to think like a terrorist when assessing your security weaknesses.

A security plan can be formatted using any structure that makes sense for your company. An example of a good model would be to structure or organize it into the following components or sections: *Personnel Security*, *Unauthorized Access*, and *En Route Security*. These areas are specifically required to be addressed by RSPA’s HM-232 rule and must be included in the plan in some form.

For each component, it is strongly recommended that you provide a complete description of the relevant specific security measures you will use to reduce your vulnerabilities. You should also discuss personnel roles and responsibilities for implementing each measure. Remember, the most effective security measures do not necessarily involve high-tech or high-cost implementations. Sometimes very simple changes in procedures can achieve the same result as a much more costly equipment-based solution.

Model security plans are available from some vendors and representatives of the hazmat transportation industry that may provide guidance for development of your plan. However, it should be noted that some plans will be more stringent than required by HM-232, and others may not adequately cover all areas addressed by HM-232. Model plans may not address the unique circumstances at each facility or for different types of trucking operations (e.g. truckload versus pickup and delivery). **You are responsible for ensuring that any model plan you use has been specifically adapted to your operations.** This is particularly true for organizations that have many sites, facilities, or terminals. A corporate-wide plan (and the accompanying security assessment) may not be specific enough to each location to be adopted outright. Additional consideration and modification will probably be necessary for each location.

Part A. Primary Security Objectives

While many security plans are developed by matching specific security measures to the vulnerabilities identified in a security assessment, we recommend taking a step back to think about what you want each security measure to accomplish. Your security plan should include specific objectives/goals and measures for your company and its employees. These are your *primary objectives*.

For example, you determine that your facility is vulnerable to a terrorist bringing a weapon into your facility. You already have a fenced facility and have located visitor parking outside the front gate. Your main goal is to prevent an armed terrorist from entering through the front gate. Your first thought may be to set up airport-type screening that includes a metal detector and an X-ray machine at the front gate. Such devices are very expensive and require a staff that is well-trained in screening procedures. There are other things you can do to achieve the same goal at a lesser expense. You could use guards with magnetic wands to detect weapons that people are carrying and they could manually inspect bags and briefcases. You may even forgo the wands and rely only on visual weapons checks. All these approaches can be equally effective with properly trained employees, yet each is progressively cheaper to implement.

A real-world example proves the value of this approach. A transit agency on the West Coast recently completed an extensive security review. It was recommended that they implement a very costly (millions of dollars) group of measures to protect their buses while they were in the yard. These included additional fencing and lighting, intrusion detection systems, extra guards and patrols, guard dogs, and more. A second review determined that all they wanted to do (their *primary objective*) was to prevent a terrorist from planting a bomb on a bus left overnight in their yard, so that it could be detonated later when the bus was in service and carrying passengers. They determined that adding a couple of new items to their existing pre-trip inspection checklist (looking in the few spaces where a bomb could be hidden that they were not already checking) would meet that objective. The cost for this procedure was minimal, saving millions of dollars.

As long as your measures meet the primary objective, you have done your job. Choosing the specific measure(s) for each primary objective can be based on any number of factors, including cost and other benefits. In the example above, there may be other tradeoffs to consider, such as the throughput that each method will allow. Many more people per hour can be screened through airport-type security devices than with manual inspection so the former may make sense for a high-volume facility.

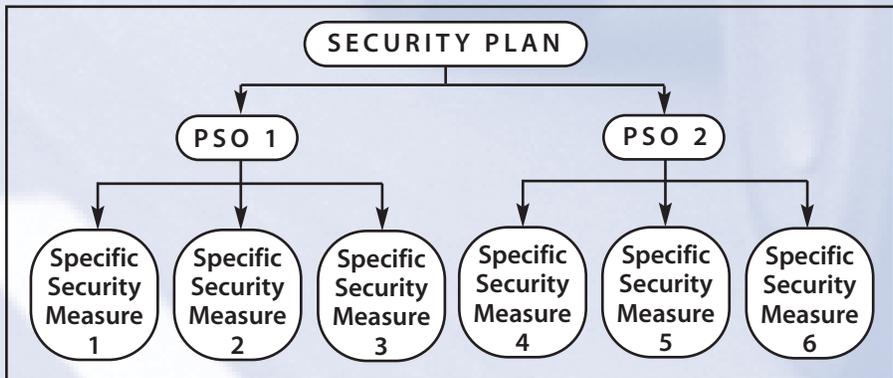
Part B. Specific Security Measures

After you identify the primary security objectives (PSOs) for each component of your security plan, you need to identify the specific security measures (or steps) you will implement to achieve each objective. A *security measure* is a policy,

procedure, device, or system that is put in place to reduce one or more vulnerabilities that you may face. If one of your PSOs is to prevent access to hazmat vehicles by non-employees, an appropriate specific security measure might be to require employee identification cards and have a security officer check cards in the area where the hazmat vehicles are parked. Another option might be to park all hazmat vehicles in a secured area and only allow access by employees with identification cards and a signed dispatch order listing a specific vehicle.

It is important to remember that specific security measures can be hardware-based (fences), technology-based (motion detection), policies and procedures oriented (always ask to see the visitor badge of anyone you do not recognize), or training-based (to reinforce policies that may not be followed properly).

The following graphic illustrates how specific security measures are related to the PSOs within a security plan. A security measure that is used to satisfy more than one PSO should be listed (by reference) in each instance and cross-referenced in the event of future changes.



As you identify PSOs and specific security measures (SMs) that are appropriate for your organization, you can use an approach similar to the one used to identify “risk” in Chapter One, Part E to select appropriate SMs. You can determine whether each PSO and the related specific SM you implement will have a high, medium, low, or very low impact (or another, similar ranking) on reducing or eliminating specific vulnerabilities. The reduction or elimination of vulnerabilities is the security benefit of that PSO and its related specific SM. Those PSOs and specific SMs that allow you to significantly reduce your vulnerabilities to the highest level of risks are those that have the greatest benefit. For example, if you are considering one SM that is extremely effective in addressing a vulnerability to a threat that, when

BENEFIT of Security Measures				
RISK	REDUCTION IN VULNERABILITIES			
	Very Low	Low	Medium	High
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	2	2

combined with your vulnerabilities and potential consequences, you have placed at the bottom of your risk ranking, you would place that SM in the bottom right cell in the table above (risk=1 and reduction in vulnerabilities=high).

Ultimately, you need to select those PSOs and specific security measures that provide the greatest benefit for the least cost. The “Prioritizing PSOs and Specific SMs” table below can provide you a way to examine the tradeoffs between cost and benefit for each PSO and its related specific SMs. You would most likely want to implement the objectives and associated measures with a value of 4 in this table (high benefit and low cost) before you would implement those with lower numbers. Your assessment of which measures are appropriate for your organization needs to consider all your vulnerabilities and that more than one measure that you are considering may address the same primary objective. In that case, you may only want to implement one of the measures and then focus on finding the best measure for another vulnerability. Of course, you may choose to assign different values to the cells in the table, but the general concept is to focus first on the measures you place in the top right—those with higher benefit and lower cost.

PRIORITIZING PSOs and SPECIFIC SMs				
BENEFIT	IMPLEMENTATION COST			
	Very High	High	Medium	Low
4	2	3	4	4
3	2	3	3	4
2	1	2	3	3
1	1	1	1	1

Part C. Addressing Varying Threat Levels

The U.S. Department of Homeland Security determines the national threat level based on information it receives from the various security organizations. The five levels of the Homeland Security Advisory System (HSAS) are color-coded based on the assessed threat condition. A *low* condition (*green*) indicates a low risk of terrorist attack; a *guarded* condition (*blue*) indicates a general risk; an *elevated* condition (*yellow*) indicates a significant risk of terrorist attack; a *high* condition (*orange*) elevates the level to a high risk; and a *severe* condition (*red*) is the highest level, indicating a severe risk of attack and requires the highest level of security.

The national threat level may be increased by one or more levels depending on the nature of any pending threats. For example, if an attack occurred under a guarded threat level (blue), the level would be immediately raised to severe (red). While it is not required that your plan address varying threat levels, it is highly recommended. Some organizations adopt a system with less than five threat levels (for example, often green, blue, and yellow are lumped into a single category, resulting in three threat levels).

Your security plan should address the specific measures or actions to be implemented for each of the threat levels. Again, some of these measures may require

only a policy change, while others may require a company to incur up-front costs at the lowest threat level to prepare for the highest threat level. You must already have the measures identified and ready to be implemented if a “red” threat condition is declared. Here is an example of why you need to think through your measures to see if there may be a problem with implementation. If your plan includes the use of off-duty police officers for security to satisfy a primary objective at orange or red threat levels, you may have a problem. When you need them most (at the red level), they are unavailable – having been assigned to perform other duties. Increased staffing needs for the police at the orange threat level may make them unavailable. Therefore, an alternative strategy or contingency plan would need to be included to address this deficiency.

When considering how to respond to varying threat levels, you should remember that the threat to your operation may be elevated for various reasons, including type of hazmat hauled or location of your facility, even if the national threat level is not raised. For example, there was a recent alert to possible terrorist threats in a state located in the Midwest but HSAS remained at yellow. Motor carriers operating in that state, however, might have implemented their plans for the orange level. Future threats and alerts could be specific to your location, as in this example, or to your industry.

Threat Conditions		Measures
LOW 	A low risk of terrorist attacks.	General measures include ensuring personnel receive proper training on the HSAS; regularly assess vulnerabilities of all facilities and regulated sectors.
GUARDED 	A general risk of terrorist attacks.	In addition to protective measures for low condition, review and update emergency procedures; check communications with drivers and employees.
ELEVATED 	A significant risk of terrorist attacks.	In addition to protective measures taken in guarded condition, increase surveillance of critical locations; implement contingency and emergency plans, as appropriate.
HIGH 	A high risk of terrorist attacks.	In addition to protective measures for elevated condition, driver should take additional precautions when stopping en route; restrict facility access to essential personnel.
SEVERE 	A severe risk of terrorist attacks.	In addition to protective measures for high condition, monitor or constrain driver travel or locations for stopping.

Some examples of general measures to address the varying threat conditions are provided in the table above [4]. A more specific example is provided at the end of this chapter.

As the table shows, with each increase in threat, additional measures are implemented. Note that while you may implement additional measures as the threat level is raised, you must be prepared for such implementation well in advance of actual implementation. When the threat is elevated, it will be too late to shop for equipment or to train employees.

Part D. Security Plan Components

As discussed above, there are three major components that must be included in your security plan in some form: personnel security, unauthorized access, and en route security. The number and extent of the measures that you choose to implement for each component is solely dependent on your analysis of your threats and vulnerabilities and your determination of the cost-effectiveness of each measure for your organization. A brief description of each component and security general objectives is provided below. More detailed examples of primary objectives and security measures for each component are included in Appendix C.

D.1 Personnel Security Component

Personnel security includes confirmation of identity and credentials. Identification of personnel is the foundation for access control, based on trust. This means a degree of confidence that an individual is who he represents himself to be and has the skills and experience claimed. Higher levels of trust relate to whether the individual can meet various operational safety and security requirements and even whether they are allowed access to secured areas or information systems. For example, to confirm the identity and credentials of job applicants, one security measure that can be used is to check the applicant's motor-vehicle record—a regulatory requirement for commercial drivers.

Personal security and safety of your personnel is an essential element of this component. This begins with the ability of the individual to recognize threatening situations, but must also be supported by systems and infrastructure that provide the capability for a proper response. For example, identifying critical personnel and establishing procedures to protect them are two security measures that you should consider adopting.

D.2 Unauthorized Access Component

How you control access to your site and to important information needs to be addressed in your plan. An example of controlling access to your site might be to install an early-warning system, such as closed-circuit television, to observe your facil-

ity externally and to actively monitor critical spaces. Another example might be installing physical barriers. Examples of controlling access to information include requiring passwords, installing a computer-intrusion-detection system, and monitoring Internet activity in your organization.

D.3 En Route Security Component

A vehicle in transit represents not just a moving target, but a critical space under constant exposure to an uncontrolled environment harboring a diversity of threats. A critical space is an area that is essential to your operations, such as a dispatch center, hazmat storage area, or an individual vehicle. When defining primary objectives, it is important to remember that the cargo is the prime source of consequential damage. Security measures that do not link directly to the regulated materials in some way, but just the vehicle, may be of limited value. An example of a security measure for en route security is regular contact with drivers, whether by telephone or by satellite tracking systems. Other security measures might be installation of bypass and shut-down mechanisms or theft-protection devices.

Part E. Example

The following example for a motor carrier with only one small facility will help illustrate the concepts presented in this chapter. We will provide some sample security measures, organized by HSAS threat level, for a primary objective related to personnel security.

Primary Objective: Prevent unauthorized people from entering facility

Sample Security Measures to Implement at Condition Green or Blue

- Implement photo employee ID badge system;
- Establish control and custody process for badges;
- Enforce display of badges for employees and visitors;
- Rely on employees to challenge unbadged individuals;
- Install a fence around facility;

- Install security guard station(s) at gate(s), but leave them unstaffed; and
- Install perimeter lighting.

Additional Sample Security Measures to Implement at Condition Yellow

- Periodically patrol the site and fence line to spot individuals not displaying their badges; and
- Occasionally test employee response to unbadged individuals.

Additional Sample Security Measures to Implement at Condition Orange

- Limit site access to one entrance and exit;
- All visitors must be escorted at all times; and
- Post a security guard at the gate.

Additional Sample Security Measures to Implement at Condition Red

- Deny visitors and vendors access to the site.

Notice that a guard gate is used at a higher threat level (orange), but needs to be installed initially, when the threat is low. Otherwise, it is too late to start constructing one in the hectic situation that will undoubtedly accompany an elevated threat. All physical or hardware-based security measures should be ready to deploy when they are needed.

If you would like to review additional examples of security measures, refer to Appendix C.

Part F. Corporate vs. Terminal Level Planning

A security plan is not a “one-size-fits-all” plan. Each plan for a site or terminal will vary based on the facility layout, design, location, highway access, and operations. In the event your company has more than one terminal, each terminal would need to have a site-specific security assessment, considering its unique characteristics. Each terminal would also need a site-specific security plan developed for and maintained at that facility. Policies or procedures may be set at the corporate level in some cases, but when implemented, may need some modification at the terminal level.

Some companies, such as chemical manufacturers, group their facilities according to the nature of their operations and the types and quantities of materials that they handle. Security planning may be done at different levels of detail for each type of facility, with the more critical facilities getting a very in-depth treatment. Some companies may wish to implement a corporate-wide security plan for each type of facility since those grouped together are very similar. This may not be appropriate! Facilities of similar size and material handling may not have similar threats and vulnerabilities. One may be in a very rural location and another may be very close to a major urban population, critical bridge, or other potential terrorist target. Local law enforcement in one area may be very proactive and effective in deterring terrorist activity and may be understaffed in another area. Also, consider the routes that hazmat vehicles take when leaving your terminals. Your facility may not be in a target-rich environment, but the routes you use may be. Site- and operation-specific analysis and treatment are always required; however, the plan you implement may still be the same.

CHAPTER THREE: SECURITY TRAINING

Security training is important to assuring the integrity of the plan, employee understanding and cooperation, and reducing the company's vulnerabilities. Security training may be categorized based on the type of information provided, level of detail, duration of the training, and level of responsibility of the employee. In addition to hazmat safety training, all hazmat employees must receive security awareness training and many of them will also require in-depth security training. Training records for each employee must be maintained with the security plan and updated as training is completed. The records must include the employee's name, the most recent training completion date, a description or copy of training materials, the name and address of the person providing the training, and certification that the employee has been trained and tested.

Part A. Security Awareness Training

There is no prescribed format for security awareness training, but it can be delivered in many forms, including classroom, CD, and over the Internet. RSPA provides an awareness training module that can be downloaded at no cost from http://hazmat.dot.gov/hmt_security.htm, or is available on CD at no charge by calling 1-800-467-4922, ext. 3.

Security awareness training is the most basic form of training and must be administered to all hazmat employees no later than the date of the first scheduled recurrent training after March 25, 2003, or by March 24, 2006. Any hazmat employee hired after March 25, 2003 must receive their security awareness training within 90 days. The awareness training must address the security risks involved with hazmat transportation, methods designed to enhance transportation security, and how to recognize and respond to possible security threats.

Part B. In-Depth Security Training

In-depth security training must be provided to each hazmat employee that is responsible for implementing or being aware of any part of the security plan by December 22, 2003. New employees hired after this date must be trained within 90 days. The training should only cover the part of the plan for which the employee is responsible. It would be poor security practice to train employees in areas for which they do not have a need to know. Training could be administered by an instructor in a classroom setting, through the use of computer modules on a CD with quizzes, or with a training video. Hazmat classification-specific training with a security component is available through various organizations or Web sites. Consult with your state or national industry association to identify resources to assist you in developing or delivering your in-depth security training.

The training material and content must include instruction or information on company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure. Use of third-party instruction materials may only augment material that is specific to your security plan. If your security plan accommodates varying threat levels, your in-depth training should inform employees of the policies, procedures, and actions expected of them at each threat level.

Part C. Recurrent Training and Recordkeeping

Currently, the hazardous materials regulations require that all hazmat employees be given recurrent training every three years on the safe handling, packaging, and transport of hazmat covered by the regulations. This training must now include security training. Additionally, the records related to employees' security training must be kept for the previous three years and for 90 days after termination of employment, as is required for other training.

CHAPTER FOUR: SECURITY PLAN ADMINISTRATION

Administration of the security plan requires a commitment from management to document its operating policies and procedures, complete a threat and vulnerability assessment, and dedicate time and resources to develop the security plan and prepare for implementation, if necessary.

Part A. Distribution and Availability

The security plan should be a written document that is secured in a location accessible to employees with the appropriate company security clearance (managers, supervisors, security officers) during the normal operating hours of the facility. The plan should not be openly distributed, but components of the plan must be available to those employees who are responsible for implementing it. Due to its sensitive nature, the plan is not a public document and should never be released to any outside party without a verified and appropriate need to know.

As with any sensitive information, it is important to develop and rigorously follow a system of logging and tracking access to the security plan. It is important to know the name of every individual who has a copy of the entire security plan and know where it is kept. It may be useful to label each page of the plan with a “plan clearance level” or similar concept that would indicate the employee type or company clearance level to which that page applies. This would help ensure that portions of the plan were not inappropriately distributed to the wrong employees.

The security plan must be made available to FMCSA investigators conducting official business as part of security contact reviews or compliance reviews.

Part B. Updates and Maintenance

Administration also includes monitoring the security plan implementation including all components, primary objectives, and specific measures to identify appropriate changes that should be considered. This activity could involve employee, vendor, and customer feedback on security measures, review of the reported security breaches, and periodic testing of security measures for weaknesses. In addition, communication to and from employees and continuous improvement to the plan, where warranted, are key elements of plan administration.

It is very important to review both the security assessment and the security plan periodically to ensure that both reflect current conditions. For large, complex companies or operations, it may be appropriate to review the assessment and the plan every year, while a review every three years may suffice for more simple operations. The assessment and the plan should be examined when the threat level changes, particularly if accompanied by specific information on the nature of the threat.

Any regulatory changes affecting any component of the plan will need to be considered and incorporated into the plan, if necessary. Of course, any revisions to

the plan must be communicated to affected employees, and all written copies must be updated simultaneously and consistently. This requires careful implementation to ensure that no old versions of the plan remain in use. One possible solution is to require the return of all old copies to a central location where they are checked off of a master list. It is good practice to include a version number and date on all pages of the plan.

Part C. Verification and Evaluation

Once you have developed and implemented your security plan, it is crucial that it is followed completely and consistently. You should establish procedures for verifying that your employees, contractors, and others are performing their responsibilities as outlined in your plan. As discussed in Part D below, you may employ outside parties, such as local law enforcement or industry partners, to assess your plan and how it is being implemented. You may also wish to test your plan with mock surveillance, phony job applicants, or other staged events to see how your plan works under actual conditions.

You should also develop performance measures for your plan to see if it is making a difference in your vulnerabilities. For example, did the new measures that you implement reduce theft or property damage? You should develop a schedule for examining the performance measures you select and assessing your plan's performance.

These steps will help you identify changes that can make your plan more effective.

Part D. Coordination, Cooperation, and Liaisons

There can be great benefit from expanding your efforts to include other partners in your security planning process. Contract carriers may wish to discuss the security of the hazmat that they transport with their shippers and consignees, particularly because they will operate within their facilities. It is important to understand how the security measures that each party implements will work with, or against, each other.

Your own industry groups are also a good source for new ideas on approaches to specific security problems and information on best practices. As discussed earlier, your industry may have developed its own guidance for you to follow. Just be sure that you are addressing the regulatory requirements as they relate to your specific operations.

An excellent source for security advice is your local law-enforcement community, including the local and state police, the FBI, and your state Bureau of Investigation. These individuals, or consultants with experience in these organizations, can be a great help in exploring your vulnerabilities as part of the security assessment. They can be used as third-party auditors to provide an independent, unbiased review of your final security plan.

APPENDIX A: UNDERSTANDING THE SECURITY THREAT

In the months following September 11, 2001, the media reported several incidents that provide real-life examples of why carriers and drivers of hazardous materials must plan and adopt security measures to prevent terrorists from commandeering their vehicles and loads. A summary of some of the incidents is provided below to assist you in understanding potential vulnerabilities and how a terrorist could acquire and use hazmat to inflict casualties or induce fear and panic. None of the domestic incidents listed have been proven to be terrorist-related, but they remain suspicious. Hijacking a tractor-trailer loaded with hazmat that could be used as a weapon of mass destruction (WMD) can no longer be dismissed. Knowing more about terrorists and their tactics can help us achieve our goal of preventing terrorist acts from occurring or succeeding.

- In Mexico, a tractor-trailer loaded with 76 drums of cyanide was hijacked on May 10, 2002. Six days later, it was recovered along with all but six drums of the cyanide. The perpetrators were only interested in the truck and not the hazmat [5].
- Two incidents in March 2003 in the U.S., within two days of each other, in the same Midwest state illustrate the potential threat posed for drivers of hazmat CMVs. First, a late-model white GMC Yukon pulled up alongside a fuel tanker truck and tried to force, at gunpoint, the truck driver to pull over. The Yukon flashed blue and red lights in its grill and had no license plates. Two days later a late-model blue Volvo with temporary Delaware tags passed a tractor-trailer on I-70. The suspicious activity of the car driver and occupant alerted the truck driver that he might be a potential target for a hijacking. A few minutes later, another car with temporary Delaware tags and two similar individuals came alongside and did the same thing. The truck driver slowed down as he neared his exit and called the state police. The car passed him and took off.
- On April 14, 2003, the FBI issued an alert in California and Oklahoma following the theft of a truck transporting 280 propane bottles. There were other reports of small propane bottles being stolen and one 500 gallon propane bottle.
- In June 2003, an Ohio truck driver pleaded guilty to two felony charges: conspiring with al Qaeda to blow up the Brooklyn Bridge and conspiring to derail a freight train.
- On May 23, 2002, a diesel fuel tanker truck departed Israel's largest fuel terminal in Haifa, Israel, for a delivery run. Terrorists planted explosives on the truck while en route, undetected by the driver. When the truck had returned to the depot and was being reloaded, a remote-controlled detonation caused an explosion and fire. The fire was barely contained before the ignition of nearby LNG tanks.

Part A. Terrorist Profiles

In a 1999 retrospective report on terrorism, the FBI classified terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorists [6]. There are many types of terrorists. Domestic terrorists may be delusional individuals (the Unabomber and Timothy McVeigh), extreme fringe groups (some animal rights and environmental groups), religious cults, or political resistance fighters (including some so-called “militias”). International terrorists may also include some of these groups, such as the religious cult Aum Shinrikyo, in addition to groups like al Qaeda [7].

To begin to think like a terrorist and, thus, identify vulnerabilities and weaknesses in your hazmat operations, you should begin with an understanding of what motivates an individual or a group to commit a terrorist act. For instance, al Qaeda is considered a special threat to United States citizens and is a group that is difficult to fight. It has the resources of a government without any of the responsibility. It is an umbrella organization with a single point of contact for multiple militant groups. It has about 700 core members from many countries and thousands of supporters all over the world. It chooses targets that are symbolic of its declared enemy, the United States. Its members are devout followers of Osama bin Laden, not just willing but eager to become the instrument of delivery in a terrorist act. such as September 11, 2001, demonstrated [7].

Part B. Terrorist Operations

B.1 Operational Acts Needed to Carry Out an Attack

Terrorist organizations, such as al Qaeda, are characterized by meticulous planning, a focus on inflicting mass casualties, and multiple and simultaneous suicide attacks. The operatives are highly trained in basic and sophisticated surveillance techniques. In fact, surveillance is only one step in a sequence of operational acts that a terrorist must complete to pull off a successful attack. These steps are the following:

- **Targeting**—terrorists first must identify a target based on their primary objectives or motivations. This could include actions designed to inflict huge casualties or significant economic disruption, attacks on facilities or buildings with significant iconic value, such as monuments, and/or actions that will result in high media exposure. Your operation may provide terrorists the equipment or materials needed to attack their target. If so, then you are a target, too!
- **Casing**—this is the careful examination of the terrorists’ plan of attack. They will think through all the steps and what might stop them. They may try to get copies of your security procedures or plan.
- **Surveillance**—a close observation of the elements of their plan. They may watch a facility to determine how many visitors, deliveries, and employees come and go and how often. Is there a regular pattern, such as during shift changes?

- Rehearsal—rarely do terrorists carry out an attack without first testing out their plan. They may stop in front of a truck to see what the driver does. They may set off your perimeter motion-detection system to test your response time.
- Attack—looks just like a rehearsal, except it doesn't end the same way. The goal of a security plan is to develop sufficient security measures to prevent them from getting to this stage at all!

The following is a list of possible indicators of terrorist casing or surveillance. The list is not exhaustive, but provides examples of suspicious activity for which hazmat carriers and their employees should be alert:

- Unusual or prolonged interest in security measures or personnel, entry points and access controls, or perimeter barriers, such as fences or walls;
- Unusual behavior, such as staring or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas;
- Increase in anonymous telephone or e-mail threats to facilities in conjunction with suspected surveillance incidents—indicating possible surveillance of threat reaction procedures;
- Foot surveillance involving two or three individuals working together;
- Mobile surveillance using bicycles, scooters, motorcycles, cars, trucks, or small aircraft;
- Prolonged static surveillance using operatives disguised as panhandlers, demonstrators, shoe shiners, food or flower vendors, news agents, or street sweepers not previously seen in the area;
- Discreet use of still cameras, video recorders or note taking at non-tourist type locations;
- Use of multiple sets of clothing, identifications, or the use of sketching materials (paper, pencils, etc.); and
- Questioning of security or facility personnel [8].

B.2 How Terrorists Pick Their Targets

The Department of Homeland Security (DHS) issued an information bulletin following the terrorist attacks in Riyadh, Saudi Arabia. The May 15, 2003, information bulletin provides potential indicators of threats involving Vehicle-Borne Improvised Explosive Devices (VBIEDs) to alert the public of possible terrorist planning and encourage the reporting of suspicious activity. The characteristic tactics used in the Riyadh attack were multiple targets, simultaneous attacks, multiple vehicles per target, and an “assault/breaching cadre” armed with small arms/weaponry accompanying the VBIED to clear security personnel and gain access for the suicide bombers.

While most non-bulk hazmat is not easily weaponized, the following classes of hazmat, when transported in sufficient quantities, are likely to be particularly attractive to terrorists because of their potential to inflict mass casualties or significant psychological trauma: explosives (Class 1); radioactive materials (Class 7); gases or liquids that are poisonous by inhalation (Division 2.3 or Division 6.1); flammable

gases or liquids (Division 2.1 or Class 3); certain organic peroxides (Division 5.2); certain biological materials (Division 6.2); and certain flammable solids (Class 4). However, other types of hazmat may also be terrorist targets because they can be used to manufacture or construct bombs or other weapons.

The most likely terrorist attack profiles for hazmat transported by commercial motor vehicle are theft, interception and diversion, and legal exploitation. For simplicity, diversion is considered a special case of interception. Theft is the taking of hazmat by means of stealth, deception, or force. Interception is the instantaneous theft with the cargo released and/or detonated or ignited while still in the control of the carrier. Diversion is a special case of interception in which the carrier is directed off its intended route and to a predetermined target. Legal exploitation would be acquiring hazmat by commercial transaction or diversion using insiders.

The attack profile used by terrorists will vary depending on such factors as the type of hazmat transported, type of transportation used, and quantity of hazmat (truckload, less-than-truckload). The target and attack profile chosen are based on the attractiveness of a specific profile relative to others, and a specific material to produce an aggregate impact outcome that maximizes the following:

- Mass casualties;
- Significant economic damage;
- Extensive psychological trauma; and
- High symbolic value.

The final determination of the attack profile a terrorist would use considers the following criteria:

- Minimal illegal activity, particularly in the early stages;
- Fewest operational acts;
- Maximizing consequences; and
- High probability of success.

APPENDIX B: ISSUES TO CONSIDER IN YOUR SECURITY ASSESSMENT

This appendix provides additional information that you may consider during your security assessment process. Not all of the issues, operations, or assets discussed will apply to your organization, but they may help you ensure that you have covered all relevant aspects of your operations. It may be beneficial to conduct your analysis without considering the protective measures that you already have in place. This will allow you to determine the vulnerabilities you have that need to be addressed. You can then examine whether your existing measures are appropriate for eliminating or reducing that vulnerability or whether less costly alternatives would do the job.

Part A. Facilities

Each physical facility used in the storage, handling, or transportation of hazmat should be analyzed for potential exploitation by terrorists. As already mentioned in this Guide, only the activities related to hazmat transportation should be considered under the requirements of HM-232. The analysis should consider the following types of facilities.

- Operations large enough to have separate headquarters are likely to use this office facility as a location for consolidation of order information. This concentration of data, including security plans, represents an attractive information-gathering target for a terrorist that is conducting casing operations (casing is discussed in Appendix A, section B.1).
- Carrier terminals are locations from where trucks are dispatched, fueled, loaded, or unloaded. Hazmat at less-than-truckload carrier terminals would be in small quantities and would not stay on site for very long. Dispatch operations are a potential source of information and can be commandeered in an effort to redirect shipments along routes to target locations as part of an attack strategy.
- Some bulk facilities are attended but unsupervised, allowing the driver to load/unload without further assistance and potentially cursory monitoring. Some non-bulk operations may present a sufficient level of activity and potential confusion to cover the diversion of material. Although the presence of hazmat at bulk carrier terminals may be rare because they often leave the terminal empty, obtain loads elsewhere, and proceed directly to the consignee, the equipment used in transport is often stored there. This would not be the case for private carriers that move their own products.
- Intermodal container shipping represents a set of vulnerabilities and security opportunities that are unique. The operational goals of speed and efficiency run counter to awareness and security, placing the security plan at risk to economic pressure. Although this will be true in all operations, it is most acutely felt at these intermodal facilities, and you might want to pay special attention to them.

Part B. Transportation Assets

Each configuration of rolling stock must be examined for vulnerabilities in light of its intended use and probable routing. Keep in mind that most vehicles represent a critical space adjacent to an uncontrolled space while they are in use. In other words, there is no moderately secure buffer zone that surrounds a truck while en route. This is the most challenging security setting.

For tractors, the issues are relatively straightforward: Who is driving? Is the person authorized to do so? Are they acting appropriately? Also, sabotaging the power units may be a concern you must address.

While the hazmat cargo is the primary concern it is usually not possible to know its status and location directly as this information is most often tied to the vehicle. You may also want to know whether a cargo tank or trailer has been separated from the power unit. You should also be concerned about devices and other contraband placed in or on the equipment to support an attack profile.

Part C. Uncontrolled Support Assets

Transportation beyond local delivery may entail the utilization of facilities owned and/or operated by others. Those facilities or types of facilities most often utilized should be an integral part of the security analysis.

Truck stops are an example where the driver will be separated from the equipment for a significant period. This is mitigated slightly by the presence of other drivers, the awareness of the truck-stop personnel, and a level of activity and mutual vigilance that can occur. To the extent possible, route selection should favor stops that provide some supplemental security in addition to that provided by the individual carriers. Rest/parking areas cannot be relied upon to provide additional security or significant opportunities for mutual support that might be enjoyed at certain truck stops. They are also generally located in remote areas far from a location where suspicious activity or actual terrorist operations could be reported.

The use of safe stopping places provides what amounts to a temporary escape from en route threats and vulnerabilities, trading these in for more predictable threats and vulnerabilities applicable to any facility. The use of a safe stopping place must, therefore, result in a net reduction in vulnerability/consequence, or the en route situation should probably continue.

Hazardous waste is hazardous material without significant economic value. Certain wastes may still possess weapons potential and should be treated as appropriate for their classification. The EPA allows transporters of hazardous waste to store manifested shipments at a transfer facility for ten days or less without being subject to their storage regulations [40 CFR 263.12]. If you use these facilities incidental to transportation, you should consider them in your assessment process.

Part D. En Route Components

Routing may present a variety of security challenges, particularly where alternate approaches or passages are not feasible or available. To the extent that routes can be identified, they should be analyzed for threats, vulnerabilities, and potential consequences (target value). You should also consider the existing FMCSA regulations on the routing of hazardous materials in your assessment of en route vulnerabilities [49 CFR 397]. These requirements include the following:

- Following state and Indian tribe routing requirements;
- Providing drivers of certain explosives with written route plans;
- Using preferred routes for highway-route controlled radioactive materials;
- Expeditiously delivering hazmat shipments; and
- Other requirements on parking and leaving vehicles unattended.

Where no other specific routing requirements apply to a shipment, FMCSA requires motor carriers to use routes that do not go through or near heavily populated areas, places where crowds are assembled, tunnels, narrow streets, or alleys, with some limited exceptions [49 CFR 397.67(b)].

Explosives, poisons, and flammables all represent significant potential consequences for weapons conversion in a tunnel scenario. Besides their target value, tunnels may also be used to facilitate a theft in a controlled environment.

Long-span bridges, such as suspension bridges, are targets for both their iconic and economic value. The investment in their construction is justified by the commercial and social benefits they provide and are often sources of great pride to the communities that surround and use them. Explosives and incendiaries would be the most likely tools of attack.

Vehicle ferries may present themselves as a target where a large number of passengers are involved, and they can be considered an opportunity to commandeer the vehicle in a controlled situation.

Gaining control of a vehicle against the will of the driver must be accomplished while the vehicle is either stopped or moving slowly. This is cause for including steep grades or switchbacks as a consideration. Downhill grades may also present a vehicle sabotage opportunity where a potential target lies below the route.

Referencing the discussion in Appendix A, part B.2, sporting and convention venues, which present opportunities as densely populated targets; government offices; and many other features near potential routes need to be considered in your assessment. From a route-selection standpoint, alternatives avoiding these potential targets should be developed to accommodate the potential for an attack occurring where the preferred route is unavailable.

Despite the best route planning, not all contingencies can be foreseen. These can be as ordinary as changes in dispatch orders due to customer direction, police and/or emergency activity necessitating route closure and detour, or unannounced construction. How the response to these situations is analyzed is important because the detour offered may be a diversion operation to place the cargo near a target or an opportunity to commandeer the vehicle. You must also consider the

routing requirements of 49 CFR 397 and any pertinent routing requirements of the states or Indian tribes' jurisdictions through which you travel. These requirements prohibit travel through or near heavily populated areas, places where crowds are assembled, tunnels, narrow streets, or alleys. Class 7 radioactive materials have even more stringent routing requirements.

Part E. Personnel

Personnel can be exploited for their information and for their responsibilities. They can provide unwitting support or be active participants in an attack operation. They can be developed as assets over months or years or become victims of sudden violence. Personnel are also the single most valuable asset in securing the operation. Technology cannot substitute for continued awareness, informed rational judgment, and responsible actions. You should address employees, contractors, vendors, and customers in your security assessment.

Businesses often underestimate the amount of information that employees possess about day-to-day operations and even strategic decision-making. Casual conversations eliciting anecdotal situations, particularly with those who have long histories with the company, can often reveal information vital to operation planning. Employees should be aware that keeping business confidence is a matter of security with consequences beyond those of a competitive nature.

Employees in otherwise good standing can also undergo life-changing events that can manifest themselves in destructive and violent behavior. Coworkers should be sensitized to indicators that someone may be vulnerable to being influenced or prone to taking violent action. Employee status changes may be used as an opportunity and cause for examining factors and researching information that can reveal potential problems.

Contractors are controlled by the language of the contract. There is a direct relationship between this language and the cost incurred; the more extensive the requirements of the contract, the greater the cost. The economic pressure must be balanced against the need to maintain your planned level of security. From a security perspective, contractors placed in positions where they can directly influence operations, or be exposed to security sensitive information, should have at least the same verifiable character as an employee placed in the same position and preferably more. In addition, contractors and subcontractors who handle hazmat that is subject to security plan requirements should be trained as to their responsibilities under the plan. For example, if a motor carrier contracts with owner-operators to perform hazmat transportation, the carrier is responsible for ensuring that each owner-operator complies with the security plan requirements applicable to their transportation of the hazmat and that the owner-operator is trained. Owner-operators, which are contract operators, provide their own transportation equipment, but the carrier that retains

them maintains certain responsibilities. Similarly, contract drivers who use company equipment also need to be trained to adhere to a carrier's security plan.

Vendors should be provided with the information needed to obtain the best price and service and nothing more. It is in the vendor's interest to obtain information about the business for marketing and strategic pricing purposes, but this does not necessarily provide the shipper/carrier with any benefit. Security sensitive information should be closely held and shared with vendors only when sufficient guarantees of confidence have been obtained and there is a strong business need, such as in the formation of a long-term partnership between shippers and carriers.

Customers can be unwitting accomplices to an attack operation. Although good customer service is usually not associated with suspicion, it is appropriate to share your security concerns with your customers. Where customers refuse to act in support of security needs, or create situations of increased vulnerability, a cost/benefit analysis of the relationship may be in order.

Part F. Information Systems

Electronic data is a great benefit as it allows the rapid transfer of important information to decision-makers. This efficiency can also be exploited. Information security must include voice and print as well as electronic data. Security planning and policy may include the following classifications for information:

- Security sensitive—such as security plans and hazardous materials orders;
- Personnel private—such as health and financial information;
- Business confidential—need-to-know business statistics and strategies;
- Commercial transaction—business-to-business that is not security sensitive;
- Workgroup shared—internally shared information; and
- Public—freely available to all.

Some organizations contract out their business systems operations, and if you do, you should consider how this affects your vulnerabilities. Does the outside firm provide sufficient security measures to prevent your information from being inadvertently released to others? What employee screening do they have in place?

Documenting order-processing procedures, including dispatch and other communication, will define the personnel who are covered by security requirements due to business processes. This will also reveal those who have access to information without any responsibility for it. Creating or modifying processes that minimize information exposure may be indicated—remember, this includes voice and print as well as electronic information.

There are two elements of internal computer information security, which would cover your personal computers, servers, local area networks, and intranets. The first is having physical access to the system; the second is having the ability to access the system to retrieve or view the information. Telephone modems are inexpensive, easily attached to a computer, and rarely accompanied by protective firewall software. These present a potential avenue for putting malicious software into the



system. E-mail and chat programs are a primary source of business communications and the most likely path that security sensitive information would take to exit the company electronically.

Many operations maintain public and private access to information over the Internet. This provides a low-cost and immediate source of information for customers and employees. The security policy should determine what content is made available. If an outside service is used to host the Web site(s), the opportunity for gaining access to unauthorized information via this offering is nearly eliminated.

APPENDIX C: SAMPLE SECURITY PLAN MEASURES

Chapter two discusses the recommended use of primary objectives to organize and select the appropriate security measures for your organization, how to vary their implementation as the security threat changes, and how to apply them to varying organizational structures. This section offers more examples on how to structure the primary objectives and select specific security measures that meet them. Again, these are offered only as limited examples and may not be appropriate or sufficient for your organization. You should develop the details of your security plan to address the vulnerabilities that you have identified in your security assessment.

Part A. Personnel Security

Personnel security includes confirmation of identity and credentials. Identification of personnel is the foundation for trust-based access control. This means a degree of confidence that an individual is who he represents himself to be and has the skills and experience claimed. This trust progresses through the ability to confirm compliance with various operational safety and security requirements to sophisticated permission systems in support of information and physical access control. Please review the graduated example below.

Primary Objective: Confirm the identity and credentials of applicants and employees

Sample Security Measures to Implement at Condition Green

- Check motor-vehicle records;
- Have a criminal background check;
- Confirm past employment;
- Confirm Social Security number; and
- Subject to drug and alcohol testing—drug or excessive alcohol use may make the individual more susceptible to blackmail or coercion.

If the applicant is applying for a driver position and will be transporting hazardous materials, additional measures should be considered that are more stringent. These measures include the requirements above and also include the following:

- Have a CDL with a current hazmat endorsement; and
- Verify citizenship.

Additional Sample Security Measures to Implement at Condition Blue

- All Hazmat employees are subject to a random check of their background and updating of their personnel files.

Additional Sample Security Measures to Implement at Condition Yellow

- All employees are subject to background checks and confirmation of the information in their personnel file; and
- Applicants are asked to provide two additional references: one personal reference and an additional reference for a former employer.

Additional Sample Security Measures to Implement at Condition Orange

- Review the personnel files of employees who were recently terminated by your company to determine if they may pose a current security threat;
- All employees must use a current credential to access workplaces (no piggybacking through access-controlled areas); and
- Interview applicants only at certain times and dates.

PERSONNEL PROTECTION

Personal physical security as well as safety is an essential component of this planning (although not covered by HM-232). This begins with the ability of the individual to recognize threatening situations. This must also be supported by systems and infrastructure that provide the capability for a proper response. Robust communications, particularly the ability to communicate as well as function under duress, are an essential consideration. Review the graduated example below. Are there other security measures you would add under a particular condition?

Primary Objective: Protect personnel deemed as critical

Sample Security Measures to Implement at Condition Green

- Determine if the organization has personnel deemed as critical;
- Establish procedures for the protection of personnel deemed critical;
- Identify and assess potential safe havens within buildings to use in emergencies (safe havens are areas that are more survivable than other areas in buildings—basements, hallways, inner rooms, or stairwells—and that generally offer a significant barrier to an intruder);
- Inform employees about buildings that contain safe havens;
- Have an emergency evacuation plan;
- Ensure the emergency evacuation plan has escape routes, emergency lighting, and exits; and
- Establish emergency lockdown/shelter-in-place procedures.

Additional Sample Security Measures to Implement at Condition Blue

- Rehearse procedures for the protection of personnel deemed critical;
- Conduct drills moving employees to designated safe havens; and
- Periodically run drills to test the emergency evacuation plan.

Additional Sample Security Measures to Implement at Condition Yellow

- Ensure that personnel are alerted and familiar with the emergency evacuation plan; and
- Ensure that personnel are familiar with emergency lockdown/shelter-in-place procedures.

Additional Sample Security Measures to Implement at Condition Orange

- Be prepared and implement the emergency evacuation plan or lockdown/shelter-in-place plans, if required.

Additional Sample Security Measures to Implement at Condition Red

- Implement protection procedures for critical personnel; and
- Implement the safe-haven plan.

Part B.	Unauthorized Access
----------------	----------------------------

Access control is usually associated with either information or an enclosed space. In either case, the basic organization and approach to defining the control strategy should be as follows:

EXTERNAL SURVEILLANCE

Primary Objective: Provide awareness of the area outside the protected space, so that early warning of possible unauthorized access is provided

Review the security measures below. What others can you think of?

- Install closed-circuit television (CCTV) to observe your facility externally and actively monitor its view of critical spaces;
- Increase perimeter lighting;
- Have security/law enforcement periodically check identified covered observation posts that can observe the site;
- Have security/law enforcement periodically check identified cover/concealment opportunities for criminals or terrorists around the site; and
- Have security/law enforcement periodically check located infiltration/egress routes for criminal or terrorist use around the site.

OBSTACLES AND BARRIERS

Obstacles and barriers provide the ability to prevent, discourage, or delay entry into the protected space at its outer boundaries. Another graduated example is provided below. Is this approach starting to make sense?

Primary Objective: Maintain a physical safety system

Sample Security Measures to Implement at Condition Green

- Install a fence around the site;
- Fenced sites should have a “clear zone” inside and outside the fence for unobstructed observation;
- Fenced-in sites should have the capability to have locked, secure gates;
- Install a security alarm system;
- Have sufficient lighting in and around the site; and
- Purchase all necessary equipment for implementation at higher threat levels. A determination will have to be made as to when to install any equipment or devices, even if not used until later. If installation is time consuming, waiting until condition orange or red may be too late.

Additional Sample Security Measures to Implement at Condition Blue

- Periodically check lighting in and around the site;
- Test the security alarm systems;
- Test the site alarm system with local law enforcement; and

- Locking hardware for gates should be case-hardened chain and high-security padlocks.

Additional Sample Security Measures to Implement at Condition Yellow

- Routinely check lighting in and around the site; and
- Rehearse actions required if the security alarm system is activated.

Additional Sample Security Measures to Implement at Condition Orange

- Activate previously installed lighting in areas not routinely covered;
- Activate the emergency law enforcement notification system; and
- Back-up automated access systems with employees.

Additional Sample Security Measures to Implement at Condition Red

- Employ additional portable lighting in and around the site for critical assets, and
- Employ obstacles or barriers in addition to standard fencing. Examples would be using concertina or razor wire to provide a double fence, or placing Jersey barriers to restrict vehicular traffic. While the concertina wire or Jersey barriers would have to already be on site, they can be put in place very quickly.

ACCESS CONTROL

Portals should allow authorized personnel, equipment and material to pass through, and exclude the passage of all else. To accomplish this filtration, it is necessary to identify those who have entrance permission. Possession, such as the use of a key, is the most passive form of confirmation, progressing to biometric and confirmation of access systems that can be real-time updated.

Primary Objective: Maintain control of everyone entering the facility

Sample Security Measures

What other measures would be appropriate for your operations?

- Determine if employee identification badges are required;
- Establish a control and custody process for the identification badge program;
- Enforce display of badge for employees while at work;
- Require photo identification badges;
- Limit site access to one entrance and exit;
- Post security guard at gate(s) if not routinely done; and
- Deny visitors, vendors, and job applicants access to the site.

INTRUSION DETECTION

The protected space should not rely totally on boundaries and access controls. Confidence in the protected space can be maintained by an awareness of activities, comparing this awareness with established norms to recognize aberrant conditions.

Primary Objective: Detect unauthorized entry into the facility

Sample Security Measures

Once again, can you come up with other measures?

- Train employees to recognize unauthorized people inside the facility;
- Institute periodic roving patrols of the facility perimeter;
- Install a property alarm system;
- Integrate alarm systems with security force and regularly exercise and check for reliability;

- Tie site alarm system into local law-enforcement department;
- Have a video camera monitor areas not under direct observation;
- Employ explosive detection devices; and
- Use metal detectors/x-ray machines to screen personnel, visitors, and bags.

COMMUNICATION AND REPORTING

Fire alarms, intercoms, dedicated communication stations and similar assets can be employed in support of detection and response protocols. These capabilities can be employed in non-traditional ways to augment security requirements. Graduated examples are listed below. Review these and, as before, see if you can develop other primary objectives and security measures that would apply.

Primary Objective: Maintain positive communication with driver

Sample Security Measures to Implement at Condition Green

- Implement a predetermined communication plan with drivers and dispatch;
- Driver and dispatcher communicate as needed via cell phone or radio; and
- Purchase equipment and plan for primary, secondary, or tertiary means of communication. As mentioned previously, a determination will have to be made as to when to install any equipment or devices, even if not used until later.

Additional Sample Security Measures to Implement at Condition Blue

- Driver and dispatch maintain regular daily communication via cell phone or radio; and
- Train with new equipment and test your plan for primary, secondary, or tertiary means of communication.

Additional Sample Security Measures to Implement at Condition Yellow

- Implement plan for primary and secondary means of communications;
- Driver and dispatch maintain communication every eight hours via cell phone or radio;
- Ensure dispatchers are familiar with drivers and their voices, and vice versa; and
- Employ radio and Internet deceptive measures for routes, times, and deliveries.

Additional Sample Security Measures to Implement at Condition Orange

- Employ tertiary means of communications to augment primary and secondary means; and
- Driver and dispatch maintain communication every four hours via cell phone or radio.

Additional Sample Security Measures to Implement at Condition Red

- Driver and dispatch maintain communication every two hours via cell phone or radio; and
- Increase frequency of GPS satellite location messages, if used, for certain high-hazard materials.

DISPATCH AND RESPONSE

The response capability should be described in terms of timing, capability, and quantity. Any response that can disrupt or otherwise degrade a potential attack scenario, without placing additional people at risk or otherwise raising the potential target value, may be considered as a security measure. Can you think of other security measures besides those listed below? What could be some primary objectives that the security measures would address?

Sample Security Measures

- Establish procedures for retaining essential employees on site;
- Have an emergency notification plan for employees (e.g., calling tree);
- Plan for emergency closure including procedures;
- When a shipment is delayed, late, or does not arrive as scheduled, have an emergency procedure in place for notification;
- Conduct drills and rehearsals with the security response force; and
- Implement predetermined alternate routes and safe stopping places as necessary.

INFORMATION SYSTEMS

The use of systems can enhance security and allows for the rapid dissemination of information. However, these systems must be secure or protected to prevent intrusion. Once again, some security measures are listed below. Develop one or more primary objectives and then use the measures below, or others you think of, to satisfy each primary objective.

Sample Security Measures

- Initiate a mass notification system for emergencies (public-address system, intercom, alarm);
- Install a computer-intrusion-detection system;
- Monitor Internet activity in your organization;
- Periodically test back-up power for communication systems; and
- Do not pass hazmat shipment data over an unsecured Internet connection.

Part C. En Route Security

A vehicle in transit represents not just a moving target, but a critical space in constant exposure to an uncontrolled environment harboring a diversity of threats. When defining primary objectives, it is important to remember that the cargo is the prime source of consequential damage. Security measures that do not, in some way, link directly to the covered materials, but just the vehicle, may be of limited value.

TRACKING SYSTEMS

Satellite systems and other technologies are excellent examples of graduated security capabilities. The frequency of location and status checks can be varied with HSAS alert levels and tailored to specific materials, reflecting the threat environment and potential consequences. A graduated example of measures is listed below. As you review it, think of what other technology is available to enhance security.

Primary Objective: Employ technology to enhance en route security

Sample Security Measures to Implement at Condition Green

- Plan for primary (phone/cell phone), secondary (radio), and tertiary (satellite tracking) means of communications;
- Install by-pass and shutdown mechanisms;
- Install panic-button option in vehicles; and

- Install theft-protection devices to disable fuel, hydraulics, and/or electrical systems;
- Seal tank trailers;
- Driver should always have a communication device readily available to him, and
- Purchase all other necessary technology devices to be installed.

Additional Sample Security Measures to Implement at Condition Blue

- Train with new equipment and test plan for primary, secondary, and tertiary means of communications;
- Routinely use primary means of communications; and
- Use high-quality hitch and trailer pin locks.

Additional Sample Security Measures to Implement at Condition Yellow

- Periodically use secondary means of communication.

Additional Sample Security Measures to Implement at Condition Orange

- Periodically use tertiary means of communication.

CARGO STATUS AND SEALS

A security plan should include measures to minimize the possibility of theft of material from a transport vehicle. Cargo seals, tamper-proof locks, and other technology may be utilized. Some cargo seals are designed to show signs of physical tampering, while others are electronic and can provide wireless notification if breached by an unauthorized individual. Note, however, that a simple locking system may be all that is necessary to deter theft. Of course, seals are not appropriate in all circumstances. For example, it would be counterproductive to use seals for bulk petroleum shipments with multiple drops (unloading).

Sample Security Measures (Can you provide more examples?)

- Check paperwork to ensure it is complete and accurate;
- Inspect cargo manifest and match with cargo;
- See that all tractor/trailer access panels/doors are locked and seals remain intact/undamaged;
- Implement a search plan for tractors and trailers on the site;
- Routinely check truck transits to ensure routing plan is on file prior to departure; and
- Arrange with consignee to notify shipper and carrier if the cargo does not reach its destination.



APPENDIX D: FMCSA SECURITY CONTACT REVIEWS

Due to the terrorist attacks committed on September 11, 2001, and subsequent threats to the transportation system, FMCSA conducted more than 30,000 security sensitivity visits (SSVs) between October 2001 and April 2002. SSVs are face-to-face meetings between FMCSA or state investigators and top carrier officials to assess security vulnerabilities and countermeasures that can improve security. FMCSA then began including SSVs as part of all compliance reviews of hazardous-materials (HM) carriers to maintain a high level of vigilance within the industry. To complement these efforts, FMCSA has initiated a new security program called a security contact review (SCR).

A security contact review is a stand-alone visit to a transportation entity that will evaluate that company's security posture. The goal is to provide assistance and recommendations for security improvements. Security contact reviews will initially be conducted at motor carriers that transport the following high-risk hazardous materials:

- Division 1.1, 1.2, 1.3, in quantities over 55 lbs. and 1.5 explosives in quantities over 1,000 lbs.;
- Division 2.3 poisonous gases in bulk packages as defined in 49 CFR 171.8;
- Class 7 highway route-controlled quantities of radioactive materials; or
- Division 6.1, packing group I materials and Division 2.1 materials in cargo tanks with a capacity exceeding 3,500 gallons.

SCRs will be ranked to focus on those carriers that transport these high-risk materials frequently and in large quantities, or who do not already have advanced security programs. For example, due to the security programs of the Department of Defense and the Department of Energy, an SCR is not necessary for carriers transporting one or more of the above materials under contract to one of these agencies. Also, a carrier that is listed as transporting Division 1.1 explosives may not transport them in quantities exceeding 55 lbs. Therefore this carrier would not warrant a SCR.

If a compliance review or safety audit is conducted on an HM carrier transporting materials warranting an SCR, an SCR should be conducted in conjunction with the review or audit.

The FMCSA investigators conducting the SCRs will complete a security contact review checklist, included at the end of this chapter. The investigator will note any regulatory violations and recommendations for enhancing security and provide them to the motor carrier.

Please note that the SCR checklist is marked as security sensitive information (SSI). This refers to a completed SCR and not the blank form. A completed SCR left with you by an investigator should be treated as you would your security plan. It should not be seen or distributed to people outside your company, or to your employees, without a valid need to know and the appropriate company security clearance.



Federal Motor Carrier Safety Administration
U.S. Department of Transportation

Security Contact Review

Company Name:

Address:

city state (2-letter) zip code

USDOT Number:

Date SCR Initiated:

at about
use arrows for start time

Select Division:

Conducted By:

SI Code: "US0000"

Note: shaded boxes indicate regulatory requirements.

IAW = in accordance with

Instructions:

- ▶ Treat this document as **Sensitive Security Information (SSI) [Need to Know Basis]**. For SSI guidelines, see **Volume II, Chapter 4, paragraph 1, subparagraph d** of the FOTM for compliance procedures for handling security information.
- ▶ All "No" responses require explanation in the comment section.
- ▶ If a question involves several parts, only check "Yes" if ALL conditions are met; otherwise, check "No" and discuss in the comment section.
- ▶ Use the company's USDOT number as the filename for this document (example: "0000000.xls");
- ▶ Append additional characters if necessary to avoid overwriting older SCRs for the same company.

Applicability

1) Does the organization fall under the provisions of 49 CFR 172.800 requiring the development and implementation of security plans?

Yes No

Comments:

Security Assessment

2) Has a specific assessment of possible transportation security risks for HM shipments been performed IAW 49 CFR 172.802(a)?

Yes No

Comments:

3) Does this Security Assessment adequately capture the specific threats and vulnerabilities faced by this organization IAW 49 CFR 172.802(a)?

Yes No

Comments:

4) Does the Security Assessment adequately capture the specific threats and vulnerabilities of personnel security IAW 49 CFR 172.802(a)(1)?

Yes No

Comments:

5) Does the Security Assessment adequately capture the specific threats and vulnerabilities of unauthorized access IAW 49 CFR 172.802(a)(2)?

Yes No

Comments:

Version 1.4

Sensitive Security Information (SSI)
[Need to Know]

- 6) Does the Security Assessment adequately capture the specific threats and vulnerabilities of en route security IAW 49 CFR 172.802(a)(3)? Yes No Comments:
- 7) Does the organization periodically assess its security posture IAW 49 CFR 172.802(b)? Yes No Comments:

Security Plan

- 8) Does the Security Plan correlate to the Security Assessment in question 2 above IAW 49 CFR 172.802(a)? Yes No Comments:
- 9) Is the Security Plan "specific" to the organization IAW 49 CFR 172.802? Yes No Comments:
- 10) Is there a written procedure on actions to take in the event of a security breach (see 49 CFR 172.704(a)(5))? Yes No Comments:
- 11) Does the organization have an Oil Spill Prevention and Response Plan IAW 49 CFR Part 130? Yes No NA Comments:

Personnel Security

- 12) Does the Security Plan contain a section addressing personnel security IAW 49 CFR 172.802(a)(1)? Yes No Comments:
- 13) Is the Security Plan's approach to personnel security operation specific IAW 49 CFR 172.802(a)? Yes No Comments:
- 14) Are the Security Plan's personnel security measures appropriate for the security assessment as written IAW 49 CFR 172.802(a)? Yes No Comments:
- 15) Are the Security Plan's personnel security measures adequate IAW 49 CFR 172.802(a) even if the security assessment did not identify all risks? Yes No Comments:
- 16) Are the Security Plan's personnel security measures being followed IAW 49 CFR 172.800(b)? Yes No Comments:

- 17) Do all drivers required by 49 CFR 383.23(a) to have valid CDLs with required endorsements have them? Yes No NA Comments:
- 18) Does the organization conduct required background checks on drivers IAW 49 CFR 391.23? Yes No NA Comments:
- 19) Does the organization take measures to confirm information provided by job applicants hired for positions that involve access to and handling of the HM covered by the Security Plan IAW 49 CFR 172.802(a)(1)? Yes No Comments:

Unauthorized Access

- 20) Does the Security Plan contain a section addressing unauthorized access IAW 49 CFR 172.802(a)(2)? Yes No Comments:
- 21) Is the Security Plan's approach to unauthorized access operation specific IAW 49 CFR 172.802(a)? Yes No Comments:
- 22) Are the Security Plan's unauthorized access measures appropriate for the security assessment as written IAW 49 CFR 172.802(a)? Yes No Comments:
- 23) Are the Security Plan's unauthorized access measures adequate IAW 49 CFR 172.802(a) even if the security assessment did not identify all risks? Yes No Comments:
- 24) Are the Security Plan's unauthorized access measures being followed IAW 49 CFR 172.800(b)? Yes No Comments:

En Route Security

- 25) Does the Security Plan contain a section addressing en route security IAW 49 CFR 172.802(a)(3)? Yes No Comments:
- 26) Is the Security Plan's approach to en route security operation specific IAW 49 CFR 172.802(a)? Yes No Comments:
- 27) Are the Security Plan's en route security measures appropriate for the security assessment as written IAW 49 CFR 172.802(a)? Yes No Comments:

Version 1.4

Sensitive Security Information (SSI)
[Need to Know]

28) Are the Security Plan's en route security measures adequate IAW 49 CFR 172.802(a) even if the security assessment did not identify all risks? Yes No Comments:

29) Are the Security Plan's en route security measures being followed IAW 49 CFR 172.800(b)? Yes No Comments:

Security Plan Administration

30) Is the Security Plan written IAW 49 CFR 172.802(b)? Yes No Comments:

31) Is the Security Plan retained IAW 49 CFR 172.802(b)? Yes No Comments:

32) Are copies of the Security Plan (or relevant portions of it) available to employees who are responsible for implementing it IAW 49 CFR 172.802(b)? Yes No Comments:

33) Are all copies of the Security Plan updated and revised as necessary to reflect changing circumstances IAW 49 CFR 172.802(b)? Yes No Comments:

Security Training

34) Does the training program contain Security Awareness Training IAW 49 CFR 172.704(a)(4)? Yes No Comments:

35) Has Security Awareness Training been provided to all hazmat employees no later than the date of the first scheduled training after March 25, 2003 or by March 24, 2006 IAW 49 CFR 172.704(a)(4)? Yes No Comments:

36) Does the Training Material contain In-Depth Security Training IAW 49 CFR 172.704(a)(5)? Yes No Comments:

37) Has In-Depth Security Training been provided to all hazmat employees with responsibility for implementing the Security Plan by December 22, 2003 IAW 49 CFR 172.704(a)(5)? Yes No Comments:

38) Does the In-Depth Security Training Material contain company security objectives IAW 49 CFR 172.704(a)(5)? Yes No Comments:

- 39) Does the In-Depth Security Training Material contain organization-specific security procedures derived from the Security Plan for personnel security IAW 49 CFR 172.704(a)(5)? Yes No

Comments:

- 40) Does the In-Depth Security Training Material contain organization-specific security procedures derived from the Security Plan for unauthorized access IAW 49 CFR 172.704 (a)(5)? Yes No

Comments:

- 41) Does the In-Depth Security Training Material contain organization-specific security procedures derived from the Security Plan for en route security IAW 49 CFR 172.704(a)(5)? Yes No

Comments:

- 42) Does the In-Depth Security Training Material contain employee responsibilities IAW 49 CFR 172.704(a)(5)? Yes No

Comments:

- 43) Does the In-Depth Security Training Material contain actions to take in the event of a security breach IAW 49 CFR 172.704(a)(5)? Yes No

Comments:

- 44) Does the In-Depth Security Training Material contain the organizational security structure IAW 49 CFR 172.704(a)(5)? Yes No

Comments:

- 45) Is the Security Training Program correctly administered IAW 49 CFR 172.704 (c) and (d)? Yes No NA

Comments:

Acknowledgement

The following company representative acknowledges receipt of a copy of this Security Contact Review

Name:

Title:

Signature: _____ Date: _____

END

APPENDIX E: REFERENCES

1. Research and Special Programs Administration, Docket No. HM-232, 68 FR 14510, available at <http://hazmat.dot.gov/68fr-14509.pdf>.
2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Title X, Section 1012, enacted by Congress October 25, 2001.
3. Transportation Security Administration, Docket No. TSA-2003-14610, Amendment No. 1572-1, available at http://www.tsa.gov/interweb/assetlibrary/68_FR_23852.pdf as of 7/3/2003.
4. Department of Homeland Security, available from <http://www.dhs.gov/dhspublic/display?theme=29>.
5. "Most of Stolen Cyanide Drums Found," available at <http://www.CNN.com/WORLD>, May 29, 2002.
6. U.S. Department of Justice, Federal Bureau of Investigation, "Terrorism in the United States 1999," 30 Years of Terrorism A Special Retrospective Edition, 1999.
7. Clayton, Bruce D., *Life After Terrorism*, (Boulder, CO: Paladin Press), 2002.
8. U.S. Department of Homeland Security, Information Bulletin 03-004, March 20, 2003.

APPENDIX F: HELPFUL INDUSTRY WEB SITES

1. American Chemistry Council (<http://www.americanchemistry.com>)
2. American Institute of Chemical Engineers (<http://www.aiche.org>)
3. American Petroleum Institute (<http://www.api.org>)
4. American Society for Industrial Security (<http://www.asisonline.org>)
5. American Trucking Associations (<http://www.trucking.org>)
6. The Chlorine Institute (<http://www.cl2.com>)
7. Commercial Vehicle Safety Alliance (<http://www.cvsa.org>)
8. Compressed Gas Association (<http://www.cganet.com>)
9. Dangerous Goods Advisory Council (<http://www.dgac.org>)
10. Federal Motor Carrier Safety Administration (<http://www.fmcsa.dot.gov>)
11. The Fertilizer Institute (<http://www.tfi.org>)
12. Institute of Makers of Explosives (<http://www.ime.org>)
13. Motor Freight Carriers Association (<http://www.mfca.org>)
14. National Association of Chemical Distributors (<http://www.nacd.com>)
15. National Propane Gas Association (<http://www.npga.org>)
16. National Private Truck Council (<http://www.nptc.org>)
17. National Tank Truck Carriers (<http://www.tanktransport.com>)
18. Research and Special Programs Administration (<http://hazmat.dot.gov>)
19. Synthetic Organic Chemical Manufacturers Association (<http://www.socma.com>)
20. Transportation Security Administration (<http://www.tsa.gov>)

