Hazardous Materials
Transportation
Security Requirements
Objectives

- Provide an overview of the security requirements found in the Hazardous Materials Regulations (HMR)
- Offer suggestions and guidance on how to comply with these requirements
Overview of the Security Requirements

- Security plan requirements
- Security awareness training
- In-depth security training
- Initial and recurrent training and record keeping
- Security plan administration
Security Plan Requirements

Each person who offers for transportation in commerce or transports in commerce one or more of the hazmat listed in 172.800(b)(1-7) must develop and implement a security plan.
Required Components of a Security Plan

• Assessment of possible transportation security threats and appropriate measures to address assessed threats

• Security plans must include the following elements:
  – Personnel security
  – Unauthorized access
  – En route security

§172.802
Required Components of a Security Plan (cont.)

• Security plans must be in writing
• Copies must be available to employees
• Plans must be revised and updated
• All current copies must be maintained
Security Plans Approved by Other Organizations

• HM-232 permits security plans that conform to regulations or standards issued by other Federal agencies, international organizations, or industry groups

• Examples may include security requirements imposed by USCG, DOD, NRC, UN, IMO, or TSA

§172.804
Security Awareness Training

- Hazmat employees must receive security awareness training at the next recurrent training, but no later than March 24, 2006
- New hazmat employees must receive security awareness training within 90 days after employment

§172.704(a)(4)
Security Awareness Training Must Include:

- Security risks associated with hazmat transportation
- Methods designed to enhance hazmat transportation security
- How to recognize and respond to possible security threats
Hazmat Transportation Security Awareness Training Module on CD-ROM

Meets security awareness training requirement as long as record keeping requirements described in 172.704(d) are followed.
In-depth Security Training

Each hazmat employee of a person required to have a security plan must be trained concerning the security plan and its implementation

§172.704(a)(5)
In-depth Security Training Must Include:

- Company security objectives
- Specific security procedures
- Employee responsibilities
- Actions to take in the event of a security breach
- Organizational security structure

§172.704(a)(5)
Other Training

Training conducted to comply with requirements of other Federal or international agencies may be used to satisfy the requirements in the HMR

§172.704(b)
Initial and Recurrent Training

- Initial training - Training must be complete within 90 days after employment or change in job function
- Recurrent training at least every three years

§172.704(c)
Recordkeeping

- A training record must be kept for each hazmat employee
- Record must include:
  - Employees name
  - Most recent completion date of training
  - Description, copy, or location of training materials used
  - Name and address of person providing the training
  - Certification of employee training

§172.704(d)
Security Plan Administration Requirements

- Plans must be in writing and retained as long as it remains in effect
- Copies, or portions of plans, must be available to personnel consistent with their need to know
- Revised/updated as necessary reflecting changing circumstances
- When update, all copies must be current as of the date of the latest revision

§172.802(b)
Overview of Suggestions and Guidance

- Hazmat security planning
  - Four step process
  - Performance standards vs. security measures
- Security threat assessment steps
- Suggested security measures
- Graduated security planning
- Example of graduated security planning
- Security plan check list
Hazmat Security Planning

Four step process:

• Assess possible security risks
• Develop *performance standards* and identify *security measures*
• Develop and implement a security plan
• Administration and training
Hazmat Security Planning

• **Performance Standards**
  – Courses of action
  – Related to threats
  – Define desired outcome

• **Security Measures**
  – Specific actions to achieve performance standards
Security Threat Assessment Steps

1. Scoping
2. Knowledge of operations
3. Assessment
4. Strategy
5. Action
6. Verification
7. Evaluation

Risk assessment guidance is available on-line at:
http://hazmat.dot.gov/riskmgmt/rmsef/rmsef.htm
Step 1. Scoping

- Determine scope of operations that need security risk management
- Characterize your hazmat transportation operations
- Identify industry partners
- Determine vulnerabilities
Step 2. Knowledge of Operations

Collect detailed information about transportation operations

• Quantities of materials transported
• Baseline security programs
• Current security procedures
• Related safety programs
Step 3. Assessment

• Analyze security threats
• Assess baseline programs
• Identify security threat control points
• Assessment may be based on:
  – Impressions of experienced staff, brainstorming, or surveys
  – Formal, rigorous hazard assessment techniques
Step 3. Assessment (Cont’d)

• “Assessment of transportation security threats” is *not* “risk assessment”
• Security is different from safety
Hazmat Safety vs. Security

Similarities
• Anticipate causes
• Avoid consequences

Differences
• Accidents can be statistically modeled
  – Intent is non-linear (not statistical)
• Frequent small vs. infrequent massive
• Safety protocols seek to prevent
• Security measures seek to reduce
Step 4. Strategy

- Rank or group security threats (low, medium, or high)
- Prioritize opportunities for security threat reduction
- Decide on preventative or control actions
- Create a written document (security plan) summarizing decisions
Step 5. Action

Implement the written plan you develop

Step 6. Verification

Monitor implementation of your strategy
Step 7. Evaluation

- Determine if goals are being met
- Identify relevant performance indicators
- Compare your strategies and results with others in your field
Required Elements of a Security Plan

- Personnel security
- Unauthorized access
- En route security

§172.802
Personnel Security

- Verify information provided on employment applications
- Ensure employees are familiar with security plans
- Encourage employees to report suspicious incidents or events
- Implement routine security inspections
- Meet regularly to discuss security measures and improve awareness
- Provide information on security issues
- Provide awareness and in-depth security training
Unauthorized Access

- Partner with local law enforcement and emergency responders
- Request review of facility
- Restrict access to facility activities and procedures
- Add security guards/off-hour patrols as needed
- Improve fencing and lighting
- Limit visitor access
- Require identification badges for staff
Unauthorized Access (cont)

- Improve security procedures for pick-up and deliveries
- Secure hazmat in locked buildings or fenced areas
- Lock vehicles and secure containers when stored at facilities
- Use tamper resistant seals and locks
- Inventory on-site hazmat periodically
- Keep records of security incidents
- Report suspicious activities to local FBI or local law enforcement
En Route Security

• Shippers know your carrier
• Identify preferred routes and alternatives
• Minimize stops
• If hazmat must be stored during transportation, ensure storage facility is secure
• Consider escorts or guards
En Route Security (cont)

- Consider using advanced technologies
- Install tamper-proof seals on valves and package or container openings
- Establish communication system
- Consignees: alert shipper if shipment is late; check carrier’s identity
- Report suspicious activities to local FBI or local law enforcement
Graduated Security Planning Using HSAS

Specific measures put into place by the plan may vary commensurate with the level of the threat at the time.

§172.802(a)
### Practical Example of Graduated Security Planning

<table>
<thead>
<tr>
<th>HSAS Level</th>
<th>Character of Planning</th>
</tr>
</thead>
</table>
| **Green** – Low | Normal operations  
 Planning and preparation |
| **Blue** – Guarded | Normal operations  
 Heightened training  
 Heightened security |
| **Yellow** – Elevated | Normal operations  
 Heightened communication/awareness  
 Increased security presence |
| **Orange** – High | Normal service delivery  
 Essential business backup  
 Modified capital and maintenance activity  
 Maximum sustainable security effort |
| **Red** – Severe | Redundant management/control  
 Modified services delivery, essential business only  
 Suspended capital and maintenance  
 Maximum surge security effort |
Security Plan “Check List”

☑ Are the “threats” adequately defined?
☑ Does the security plan address the “threats”?
☑ Does the security plan define “performance standards”?
☑ Are the security measures site specific?
☑ Are the security measures appropriate to the operation, the threats, and the performance standards they are intended to support?
☑ Are the defined threats, performance standards and their supporting security measures adequate to the operation?
Remember...

- Think prevention
- A security plan is not an emergency plan – it is supposed to *reduce the potential*, as well as mitigate consequences, of a security related incident
- Most effective measures don’t always involve high-tech or high-cost solutions
- A security plan is not a “silver bullet”
Informational Resources

http://hazmat.dot.gov
How Can You Reach Us?

Hazardous Materials INFO-LINE
1-800-HMR49-22
(1-800-467-4922)
Hours of Operation: 9 am – 5 pm EST

– Obtain answers to HMR questions
– Request copies of Federal Register, exemptions or training materials
– Report HMR violations
– Fax on Demand

E-mail: infocntr@dot.gov
Got A Question?