Outline

I. Specific requirements of HM-232
II. How to Comply: Suggestions and Guidance

Part I - Overview

- Summary of HM-232 requirements
- Security awareness training
- Security plan requirements
- In-depth security training
- Administration – training and record keeping
- Security plan administration
Summary of HM-232 Requirements

- Security awareness training
- Security plans
- In-depth security training

Security Awareness Training – 172.704(a)(4)

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.

Security Awareness Training Must Include:

- Security risks associated with HM transportation
- Methods designed to enhance HM 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.

Security Plan Requirements – 172.800

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

Required Components of a Security Plan – Part 172.802

- 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
Required Components of a Security Plan (Cont’d)

- 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

In-depth Security Training – 172.704(a)(5)

Each HM employee of a person required to have a security plan must be trained by December 22, 2003
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

Other Training

Training conducted by:

- OSHA
- EPA
- Other Federal or international agencies

may be used to satisfy training requirements in 172.704(a)

Administration

- Recurrent training at least once every three years
- Record of current training must be created and retained
Recordkeeping

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

Security Plan Administration Requirements

- Plans must be in writing
- Must be in place by September 25, 2003
- Copies must be available to personnel
- Must be revised and updated
- Revised/updated copies must be maintained

Part II - Overview

- HM 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
HM 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

- Performance Standards
  Courses of action
  Related to threats
  Defines 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/rmsef
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

HM 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

**Suggested Measures**
Measures that may be implemented as part of a security plan:
- Personnel security
- Unauthorized access
- En route security
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’d)

- 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

En Route Security (Cont’d)

- Consider escorts or guards
- 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.

49 CFR 172.802(a)


Practical Example of Graduated Security Planning

<table>
<thead>
<tr>
<th>HSAS Level</th>
<th>Character of Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green – Low</td>
<td>Normal operations</td>
</tr>
<tr>
<td>Blue – Guarded</td>
<td>Normal operations, heightened training</td>
</tr>
<tr>
<td>Yellow – Elevated</td>
<td>Normal operations, heightened communication/awareness</td>
</tr>
<tr>
<td>Orange – High</td>
<td>Normal service delivery, business backup</td>
</tr>
<tr>
<td>Red – Severe</td>
<td>Redundant management/control, modified services delivery, essential business only</td>
</tr>
</tbody>
</table>

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”
Available Information Resources

- training@rspa.dot.gov
- Order publications on-line at http://diy.dot.gov/hazmat
- Information Center – (800) 467-4922 (9 a.m – 5 p.m. ET)

Questions?