SECURITY IN MANUFACTURING, TRANSPORTATION, STORAGE AND USE OF COMMERCIAL EXPLOSIVES
Member Companies (As of March 2019)

Accurate Energetic Systems, LLC
McEwen, Tennessee

Austin Powder Company
Cleveland, Ohio

Baker Hughes, Inc. (a GE Company)
Houston, Texas

Davey Bickford USA, Inc.
Sandy, Utah

Detotec North America, Inc.
Sterling, Connecticut

DYNAEnergetics, US, Inc.
Austin, Texas

Dyno Nobel, Inc.
Salt Lake City, Utah

General Dynamics - OTS - Munition Services
Joplin, Missouri

GEODynamics, Inc.
Millsap, Texas

Hilltop Energy, Inc.
Mineral City, Ohio

Hunting Titan
Milford, Texas

Jet Research Center/Halliburton
Alvarado, Texas

Maine Drilling & Blasting
Auburn, New Hampshire

Maxam North America
Salt Lake City, Utah

MP Associates, Inc.
Ione, California

Nelson Brothers, Inc.
Birmingham, Alabama

Nobel Insurance Services
Dallas, Texas

Orica USA, Inc.
Watkins, Colorado

Owen Oil Tools LP
Godley, Texas

R.A. McClure, Inc.
Powell, Ohio

Safety Consulting Engineers
Schaumberg, Illinois

Senex Explosives, Inc.
Cuddy, Pennsylvania

Special Devices, Inc.
Mesa, Arizona

Teledyne RISI
Tracy, California

Tread Corporation
Roanoke, Virginia

Vet’s Explosives, Inc.
Torrington, Connecticut

Visible Assets
Stratham, New Hampshire

W.A. Murphy, Inc.
El Monte, California

Liaison Class Members

Association of Energy Service Companies
Friendswood, Texas

Australian Explosives Industry & Safety Group (AEISG)
Tweeds Head, Australia

Brazilian Association of Explosive and Aggregate Materials Industries (ABIMEX)
Sao Paulo, Brazil

Canadian Explosives Industry Association (CEAEC)
Ottawa, Ontario, Canada

Explosives Safety & Technology Society - Visfotak
Maharashtra, India

Federation of European Explosives Manufacturers (FEEM)
Brussels, Belgium

International Society of Explosives Engineers (ISEE)
Cleveland, Ohio

National Institute for Explosives Technology (NIXT)
Lonehill, South Africa

SAFEX International
Christiansted, South Africa
IME is a nonprofit association founded in 1913 to provide accurate information and comprehensive recommendations concerning the safety and security of commercial explosive materials. IME represents U.S. manufacturers and distributors of commercial explosive materials and oxidizers as well as other companies that provide related services. Although our member companies are based in North America, IME members operate globally with operations and distribution points on all continents except Antarctica.

IME was created to provide technically accurate information and recommendations concerning commercial explosive materials and to serve as a source of reliable data about their use. Committees of qualified representatives from IME member companies developed this information and a significant number of their recommendations are embodied in the regulations of state and federal agencies.

The Institute’s principal committees are: Environmental Affairs, Government Affairs, Legal Affairs, Safety and Health, Security, Technical, and Transportation and Distribution.
TABLE OF CONTENTS

FOREWORD ........................................................................................................................................... 1
DEFINITIONS ........................................................................................................................................... 2
GENERAL SECURITY CONCEPTS ..................................................................................................... 3
SPECIFIC RECOMMENDATIONS ....................................................................................................... 5

SECTION I – MANUFACTURING ...................................................................................................... 5
A. General Access Control for Permanent Facilities ................................................................. 5
B. Entrances ..................................................................................................................................... 5
C. Explosives Production Facilities .......................................................................................... 5
D. Inventory Control and Recordkeeping of Precursor Chemicals and Finished Goods .............. 5
E. Intraplant Transportation ...................................................................................................... 5
F. Disposal of Explosives ........................................................................................................... 6
G. Visibility or Ground Clearance .............................................................................................. 6
H. Plant Utility Systems ................................................................................................................ 6
I. Plant Evacuation ..................................................................................................................... 6

SECTION II – SALES AND DISTRIBUTION .................................................................................... 6
A. Sales of Explosives ................................................................................................................... 6
B. Use of For-Hire Carriers ......................................................................................................... 7

SECTION III – TRANSPORTATION OF CLASS 1 MATERIALS (UNLESS OTHERWISE MENTIONED) ........................................................................................................................................ 8
A. Security Plans and Training .................................................................................................... 8
B. Loading ..................................................................................................................................... 8
C. Unloading ............................................................................................................................... 8
D. Highway ................................................................................................................................... 8
E. Water ....................................................................................................................................... 10
F. Rail ......................................................................................................................................... 12

SECTION IV – STORAGE .................................................................................................................. 13
A. Site Control ............................................................................................................................. 13
B. Frequency of Inspection .......................................................................................................... 13
C. Magazines .............................................................................................................................. 13
D. Vehicular Magazines (Bulk Trucks, semi-trailers, van trucks) ............................................. 13
E. Keys and Locks ....................................................................................................................... 14
F. Inventory recordkeeping ....................................................................................................... 14
G. Reporting Loss or Theft ......................................................................................................... 14
H. Visibility or Clear Area ......................................................................................................... 14
I. Access .................................................................................................................................... 15
J. Reconciliation ......................................................................................................................... 15
K. Storage of Binaries ............................................................................................................... 15
SECTION V – USE ............................................................................................................................... 16
A. Blast Site Security .......................................................................................................................... 16
B. Blast Records ............................................................................................................................... 16
C. Conduct in Public .......................................................................................................................... 16
D. Attendance of Explosive Materials ............................................................................................ 16
E. Unused Explosives ......................................................................................................................... 16
F. Blasting Permits ............................................................................................................................. 16
G. Licensed or Certified Blaster .......................................................................................................... 17

SECTION VI - SECURITY MEASURES DURING ELEVATED THREATS (AND DISASTERS).............................................................................................................................. 18
A. Perimeter Protection/Access Control .......................................................................................... 18
B. Communication ............................................................................................................................ 18
C. Manufacturing ............................................................................................................................. 19
D. Sales and Distribution ............................................................................................................... 19
E. Use ................................................................................................................................................ 19
F. Oil and Gas Operations .............................................................................................................. 19
G. Storage Sites and Portable Magazines on Job Sites ................................................................. 20

APPENDIX A – EXAMPLE FIXED SITE SECURITY PLAN ................................................................. 21
APPENDIX B – RECOMMENDED ELEMENTS OF A TRANSPORTATION SECURITY PLAN .................................................................................................................. 27
APPENDIX C – SAMPLE QUESTIONS WHEN ASSESSING YOUR VULNERABILITY .......... 29
APPENDIX D – SECURITY CLASSIFICATIONS IDENTIFICATION .............................................. 31
APPENDIX E – CYBER SECURITY MEASURES ............................................................................. 32
APPENDIX F – TRAINING ................................................................................................................ 34
APPENDIX G – RISK ASSESSMENT ............................................................................................... 35
SAFETY LIBRARY PUBLICATIONS ................................................................................................. 37
SLP-27
Security in Manufacturing, Transportation, Distribution, Storage and Use of Commercial Explosives

This SLP cannot and is not intended to cover all potential security risks or all appropriate responses to security threats facing the explosives industry. Rather, the information and recommendations provided in this SLP are intended to assist and inform users of explosives and those in the explosives industry to identify and assess potential security vulnerabilities, and to devise company-specific plans to prepare for and respond to security alerts and threats.

FOREWORD

Since its inception in 1913, the Institute of Makers of Explosives (IME) has recommended that explosives be stored in theft-resistant magazines under lock and key. Safety Library Publication (SLP) 27 provides recommended guidelines for security in the manufacturing, transportation, storage and use of commercial explosives and their precursor chemicals.

The commercial explosives industry, long aware that explosives and precursor chemicals can be attractive to criminals, operates at an elevated security level. Regulatory requirements and industry best practices have largely prevented diversion of commercial explosives for illicit purposes or use as components of improvised explosives devices. While the recommendations in SLP-27 are applicable to everyday operations, IME stresses that the best practices included herein are especially critical to operations involving detonators.

SLP-27 also makes recommendations for time periods when the Department of Homeland Security (DHS) issues threat alerts using its National Terrorism Advisory System (NTAS). Enhanced security measures are intended to be implemented in specific geographical areas, markets or industry segments facing a potential or immediate security threat, as designated by DHS or other governmental agencies. Individual manufacturers, distributors and users should develop action plans with enhanced security measures to be implemented in the event of increased threats.

Although reference may be made to federal security regulations, a deliberate effort was made to provide recommendations that do not repeat the regulations. Where federal regulations are repeated in this document, terms such as “must”, “will”, and “should” are used. All federal, state and local laws and regulations regarding explosive manufacturing, transportation, storage, sales, use, and disposal must be strictly adhered to. Other IME SLPs should also be consulted for additional, detailed information that may be appropriate. Safety Library Publications are available for free download at www.ime.org.
DEFINITIONS

Definitions of terms used in this document can be found in IME SLP-12, *Glossary of Commercial Explosives Industry Terms.*
GENERAL SECURITY CONCEPTS

This section describes general commercial explosives industry security practices and viewpoints that are difficult to explain in regulatory-style language. Readers should think about how these generalizations fit into their operations.

A. Limit public disclosure of information on quantities and locations of explosives storage except that public safety authorities such as fire, police, and local emergency management should be in possession of specific information regarding the quantities and location of explosives storage facilities.

B. Get to know the local law enforcement, emergency responders and Joint Terrorism Task Force in your area and get them to know you. Holding an annual “open house” at your facility is recommended to accomplish this. This not only allows law enforcement and emergency responders to gain first-hand familiarity with your facility, but also provides invaluable face-to-face interaction with these authorities. If you cannot get law enforcement or emergency responders to visit your facility, visit them. Request a meeting so you can introduce and explain your operations. Specifically request in writing that law enforcement pay special attention to any suspicious activity around your site(s).

C. Instruct all employees to report any unusual or suspicious activity to appropriate authorities immediately; WHEN IN DOUBT POINT IT OUT. Such activity could include:
   1. an attempt to purchase explosives or precursor chemicals by an unfamiliar or seemingly inexperienced individual;
   2. an individual who is reluctant to provide identification or information on their operation or intended use of explosives;
   3. encountering an individual, either at work, on your own time or online, who seems very interested in your occupation and/or details related to the accessibility of explosives, blasting agents, or precursor chemicals;
   4. out-of-place or repeat sightings of vehicles\(^1\) or individuals in vicinity of your facilities or at facility gates or perimeter roads and aerial over flights including unmanned aerial systems (UAS) or drones;
   5. sighting unauthorized individuals inside a secure area within your facility; or
   6. following or surveillance of vehicles used by the explosive industry.

D. Write down information such as date, time, vehicle color, make, license number and state, and physical description of individuals as soon as possible after becoming suspicious of them. Take a photograph if possible, and soon after, send it to a company e-mail address where it can be securely stored, retrieved and sent to authorities if necessary. Retain and preserve papers or other items a suspicious individual may have touched for potential law enforcement processing. When witnessing known criminal activity, contact law enforcement immediately.

E. Designate an individual as your security coordinator. All employees should report suspicious or unusual activities to the security coordinator or their immediate supervisor if the security coordinator cannot be contacted. The security coordinator or supervisor then reports the suspicious or unusual activities to appropriate law enforcement personnel. The

\(^1\) When the term “vehicle” is used it includes freight containers mounted on flatbed trucks.
security coordinator should also establish relationships with nearby chemical operations to share information. The security coordinator should maintain a log of unusual events.

F. Establish a predetermined action plan for implementation of increased security measures brought about by an NTAS Alert. Procedures within the action plan addressing shipments, production, and blasting operations in progress should be well understood by all employees. In the event of an NTAS Alert, additional security measures should be considered for implementation on a site-specific basis, in view of the type and scope of the specific alert.

1. Disseminate increased security alerts and security recommendations such as these to your customers and suppliers throughout the industry. Facilitate their understanding of these alerts and recommendations.

2. Control official documents and information. Prevent documents such as licenses, permits, route plans, shipping schedules and other authorizations from reaching unauthorized individuals. Information related to shipping, inventory, production schedules, and processes should be kept secure and provided on a need-to-know basis.

G. Conduct periodic safety and security reviews of all outside contractors or service providers who have access where explosives or sensitive documents are located. All contractors and outside service providers should be escorted in areas where explosives are accessible. Include a security element in contractor or service provider indoctrination training.

H. Develop security plans and conduct vulnerability assessments for your entire operation. A sample security plan can be found in Appendix A. Examples of questions to ask in a vulnerability assessment can be found in Appendix B. Several sources of information on vulnerability assessments may be found at:

1. DHS’ Voluntary Chemical Assessment Tool
   http://www.dhs.gov/files/programs/gc_1260467577301.shtm


3. National Institute of Justice’s A Method to Assess the Vulnerability of U.S. Chemical Facilities

4. TSA’s Exercise Information System (EXIS)

I. Subscribe to and monitor the Department of Homeland Security Information Network Website (HSIN) for daily activity pertaining to security issues around the country.
SPECIFIC RECOMMENDATIONS

SECTION I – MANUFACTURING

A. General Access Control for Permanent Facilities
   1. Fences and Gates – Where high explosives are manufactured the facilities should be enclosed by fences with gates capable of being locked. Other security measures, such as cameras or UAS, may be considered in lieu of fences or gates. Similar security measures are encouraged for the manufacturing of other classes of explosives.
   2. The integrity of the fences and gates should be checked routinely.

B. Entrances
   1. The number of entrances should be limited to the minimum number necessary to conduct operations.
   2. Entrance to the facility should be controlled and restricted only to those authorized for access.
   3. Entrances should have a gate or other barrier that requires a vehicle to stop.
   4. Identification, Vetting and Credentialing
      a. All employees should wear photo or other corporate ID badges where they do not cause a safety hazard or where visual recognition is not feasible. (See Appendix D)
      b. Visitors should always wear ID badges. (See Appendix D)
      c. Each visitor should individually sign in and out of the facility.
      d. Each site should have a system to verify compliance with section e.
      e. Prepare and maintain a current list of all employees, home addresses, telephone numbers, and emergency contacts. The list may contain vehicle types and license numbers.
   5. Firearms or other potential weapons are not permitted on the facility without prior written authorization of the most senior person responsible for the operation of the facility (or their designee in their absence), unless applicable law dictates otherwise.

C. Explosives Production Facilities
   1. Entry – Personnel should not enter, remain in, or go near explosives manufacturing buildings unless it is necessary for the performance of their duties.
   2. Visitors’ access to production facilities should be limited to authorized individuals only and visitors should be escorted in designated areas. See Appendix C for additional guidance.
   3. Attendance
      a. All buildings containing in-process explosives and precursor chemicals should be locked or attended by production workers.
   4. Parking – Visitors should park in designated areas only. These areas should be clearly marked.

D. Inventory Control and Recordkeeping of Precursor Chemicals and Finished Goods
   – Inventory accountability procedures and accurate inventory records should be maintained.

E. Intraplant Transportation
   1. Documentation should record the type and quantity of explosives or precursor chemicals for each movement.
   2. Only authorized personnel should move explosives or precursor chemicals within the facility.
F. Disposal of Explosives
   1. Security for the on-site disposal of explosives should be the same as that applied to explosive manufacturing processes.
   2. Security for the off-site disposal of explosives should be the same as that applied to the sales and distribution of explosives.

G. Visibility or Ground Clearance
   1. At a minimum, the ground within 10 feet (3.05 m) of any fence or gate should be maintained to provide a clear field of view.
   2. No large trees or sloped embankments that could allow access over the fence or gate should be permitted.

H. Plant Utility Systems
   1. Plant utility systems such as water wells, tanks, pump stations, electrical substations, gas lines, fuel storage areas, and raw material pipelines, should be locked to prevent tampering or unauthorized access and should be inspected periodically. An inspection log should be maintained.
   2. Electrically powered security equipment should have a backup on-site power source.

I. Plant Evacuation
   1. Procedures consistent with OSHA’s emergency action plan standard in 29 CFR 1910.38 should be in place.
   2. The plant emergency action plan and emergency control manual should be maintained and reviewed at least annually.
   3. Where a building could not be secured during an emergency evacuation, upon return, verify that explosive materials have not been tampered with or removed without authorization.

SECTION II – SALES AND DISTRIBUTION

A. Sales of Explosives – A “Know Your Customer” program should be established. Such a program should include:
   1. Verification required before any/all sales:
      a. A certified copy of the customer’s current ATF license or permit,
      b. A list of the customer’s employees authorized to accept delivery of explosives on behalf of the customer, and
      c. A certified statement of intended use by the customer.
   2. Other components:
      a. Consider any abnormal circumstances in a transaction that indicate that the explosives may be destined for an inappropriate end-use, end-user, or destination.
      b. Confirmation that customer is not listed on screening lists such as those published by the Department of Commerce, Department of State, and Treasury Department1. Although specifically directed at exports, these lists can be helpful in identifying persons and companies in the U.S. with possible terrorist links.

1 A consolidated search engine that searches 11 such lists is available at: https://www.export.gov/csl-search
B. Use of For-Hire Carriers

1. Procedure for missing or delayed explosives – A procedure should exist that establishes a notification process between the carrier and the shipper in the event explosives are missing or delayed while in the care of the carrier.

2. Verification of delivery – Verification of delivery of explosives should be made to confirm receipt of all items.

3. Shipper’s Review of Motor Carrier – If the shipper uses for-hire motor carriers, the shipper should review the carriers’ qualifications to transport explosives prior to the first shipment and periodically thereafter. At a minimum, this review should include:
   a. A copy of the carrier’s Pipeline and Hazardous Materials Safety Administration Certificate of Hazardous Materials Registration and state hazmat registration(s) and/or permit(s), if applicable
   b. A copy of their last Federal Motor Carrier Safety Administration (FMCSA) Compliance Review, if applicable. If the FMCSA review was conducted more than 5 years ago, if possible, conduct your own or have the carrier request one for your review later. The carrier must have a “satisfactory” rating
   c. A review of the carrier’s FMCSA Comprehensive Safety Analysis (CSA) score.
   d. A copy of the carrier’s FMCSA Hazardous Materials Safety Permit, if applicable.
   e. A copy of the carrier’s insurance including federal financial responsibility endorsements
   f. Certification by the carrier that it has a DOT compliant security plan.
   g. The carrier’s emergency response procedures as they relate to the movement of the shipper’s products
   h. Complete listing of carrier contacts, both business and after business hours, and
   i. Verification that elevated threat protocols based on NTAS Alerts have been established for Class 1 materials (explosives) and Class 5 materials (oxidizers) identified in TIER 1 & 2 Hazardous Security Sensitive Materials (HSSM)
SECTION III – TRANSPORTATION OF CLASS 1 MATERIALS (UNLESS OTHERWISE MENTIONED)

A. Security Plans and Training
   1. Shippers and carriers must have security plans and security training compliant with governing regulations.
   2. As part of a pre-trip inspection, drivers should be trained to identify anything suspicious or out-of-the-ordinary either in or on their vehicle and report to their supervisor prior to departing.

B. Loading – Customer names or destinations should not be displayed on scheduling boards in areas where the public or unauthorized employees have access.
   1. Storage – Explosive materials should be removed from storage, prepared for shipment, and transported to the destination without unnecessary delay.
   2. Manufacturing – When explosives are manufactured and immediately prepared for shipment, procedures should be in place to prevent unauthorized movement of the explosives.

C. Unloading – Once reaching their destination, Class 1 materials should be unloaded into proper storage or used upon arrival.

D. Highway
   1. International Shipments
      a. National border crossings – Carriers should participate in the U.S. Customs and Border Protection Free and Secure Trade (FAST) program.
      b. Border crossings – Vehicles should avoid high-volume border crossings where long delays frequently occur. Long delays are two hours or more time waiting in traffic and processing paperwork. If border crossings where long delays occur must be used, contact the authorities of both countries to obtain the procedures necessary to expedite the border crossing.
         i. Time of day – Vehicles should cross borders during low volume times of the day
      c. Documentation – All permits and documentation should be completed prior to materials arriving at the border crossing
      d. Explosives handling – No handling of Class 1 materials other than for customs inspection should be conducted at the border crossing. To the extent possible, cargo should be pre-cleared, and containers or trailers should be sealed
   2. Cross-docking and Trailer Transfers – Cross-docking and transfer of trailers to other carriers should be done in secure areas
      a. Safe havens for commercial explosives
         i. In the event of an applicable NTAS Alert, vehicles transporting Tier 1 and 2 HSSM explosives should seek refuge at the nearest safe haven or take other security measures identified by the employer, which may include law enforcement escorts or refuge at an industry affiliate location.
         ii. NFPA 498 - Safe havens should be operated in accordance with the most recent edition NFPA 498 or other comparable operating procedures approved by a local authority having jurisdiction (AHJ).
         iii. Commercial safe haven review – The carrier’s safety department should review and approve the commercial safe haven location, authorization, and operation procedures prior to using it.
   3. Congestion – Congested areas and rush hour traffic in large cities should be avoided if possible.
4. Parking and Stopping Vehicles
   a. The parking of vehicles containing Division 1.1, 1.2, 1.3, 1.4, or 1.5 materials must comply with 49 CFR Part 397.7.
   b. All non-traffic stops, parking locations, and layovers should be kept to a minimum.
   c. The explosives and vehicles should be secured from unauthorized access or use at all times.

5. Attendance of Vehicles -- All employees should be instructed to immediately report any unusual or suspicious activity to appropriate authorities.
   a. Vehicles transporting Division 1.1, 1.2, and 1.3 materials must be attended at all times.
   b. Attendants must be qualified as follows:
      i. Made aware of the class of explosive materials in the motor vehicle and of its hazards;
      ii. Instructed in the measures and procedures to be followed in order to protect the public from such hazards;
      iii. Familiarized with the vehicle assigned to attend; and
      iv. Trained, authorized, and enabled to move the vehicle when required.
   c. Definition of “attended” – For the purpose of this section, a motor vehicle is deemed “attended” only when an attendant:
      i. Is physically on or in the vehicle, and not in the sleeper berth, or is within 100 feet, and has the vehicle within his unobstructed field of vision, and can reach it quickly without any interference; and
      ii. Is awake and alert and not engaged in other duties or activities which divert attention from the vehicle.

6. Locking or Sealing of Cargo
   a. All cargo compartments containing Class 1 materials should be locked or secured with a seal.
   b. If seals are used, the seal numbers should be recorded on the shipping papers.

7. Shipping Documents – Documents and shipping information should be kept in a pocket on the driver’s door or within his reach when the driver is in the vehicle. When the driver is out of the vehicle, shipping papers should be in the driver’s door pocket, or on the driver’s seat.

8. Route or Trip Plans
   a. A route or trip plan should be prepared for all placarded shipments of Class 1 materials. A route plan must be prepared for Division 1.1, 1.2 and 1.3 shipments consistent with 49 CFR 397.67(d)
   b. The route or trip plan should include all stops
   c. Avoid patterns on routes, departures, and stops
   d. HAZMAT preferred routes should always be considered when making route plans.
   e. Hazmat restricted routes may only be used when permission is granted by the AHJ
   f. Under NTAS elevated threats, security risks may supersede safety risks and this determination will be made by the carrier using a risk-based analysis

9. Team Driver Program – Two drivers should be used for delivery of Division 1.1, 1.2 and 1.3 materials with destinations that cannot be completed by a single driver without taking a layover

10. En Route Communication
    a. Equipment - All vehicles transporting Class 1 materials should be equipped with a means of two-way communication and/or two-way GPS systems. Shipments of Class 1 materials that take more than a single driver’s hours- of-service to complete should
be monitored with a communication and tracking system similar to a GPS-based communication system.

b. Communication Plan - Carriers transporting Division 1.1, 1.2, and 1.3 materials must have a communication plan consistent with 49 CFR 385.407(b)(2).

c. Frequency
   i. Drivers should communicate with dispatch at predetermined stops as detailed in route or trip plans and upon arrival and departure from destinations when laden with Class 1, Division 1.1, 1.2 and 1.3 materials.
   ii. Drivers transporting Class 1, Division 1.1, 1.2, and 1.3 materials must make contact with dispatch consistent with 49 CFR 385.415(c)(1).

11. Physical Security of Vehicles – A secure battery disconnect switch, Steering wheel lock, air brake locking mechanism or other appropriate locking control processes, or a combination thereof should be installed or available in all vehicles that transport Class 1 materials.

12. Breakdowns and Incidents
   a. Mechanical Breakdowns
      i. In case of a mechanical breakdown, drivers should contact dispatch immediately.
      ii. In the event of mechanical breakdowns, drivers should move the vehicle to the safest possible location. Drivers should stay with their vehicles until such time that the necessary repairs are made to continue the trip or await another vehicle to transload cargo if the vehicle cannot be repaired at roadside.

   b. Incidents - If involved in an accident or incident, the driver should contact dispatch and state law enforcement when it is safe to do so.

   c. Rendering aid - Drivers should not stop to give aid to other vehicles stopped or involved in accidents or incidents. These situations should be reported to the proper authorities when it is safe, secure and compliant with relevant laws and regulations.

E. Water

1. Staging – Division 1.1, 1.2, and 1.3 materials awaiting conveyance to another mode or means of transport should be secured in a safe haven or in an area designated by the Captain of the Port (COTP).

2. A Responsible Safety and Security Individual (RSSI) should be present at all times when Division 1.1, 1.2, and 1.3 materials are being handled at the berth.
   a. Qualifications - A RSSI should be:
      i. A representative of (either) the
         1. shipper for exports; or
         2. consignee for imports
      ii. Trained and experienced in explosive safety and security, port operations, and explosives handling;
      iii. Knowledgeable of the applicable regulations;
      iv. Knowledgeable of the Class 1 materials being handled; and
      v. Knowledgeable of how to handle broken or damaged packages or any spillage of Class 1 materials.
   b. An RSSI must possess a transportation worker identification credential (TWIC®).

3. Emergency Response Plans
   a. Emergency response plans for incidents on ships, on commercial waterfront facilities, and in port areas should be consistent with those described in 29 CFR 1910.120 (q) and 33 CFR Parts 101-105, as applicable.
   b. Emergency response plans should be reviewed after each exercise, emergency, or when changes are made in the port that would affect the existing plan.
   c. RSSI responsibilities -- the RSSI should be familiar with local emergency response plans and should notify local authorities, coordinate activities and
report them as required by the emergency response plan.

d. Facility Operator Responsibilities
   i. Facility operators should notify the pertinent local authorities of the net explosive quantity and the expected handling date(s) at least 24-hours in advance.
   ii. The commercial waterfront facility operator should develop an emergency response plan for the commercial waterfront facility.
   iii. A copy of the facility emergency response plan should be provided to the RSSI, port authority, regulatory authority, and master of the ship by the facility operator.

e. Vessel Operator Responsibilities
   i. The master should maintain the vessel in a state of readiness and provide enough personnel on board the vessel, so as to be able to affect immediate departure, should the need arise.
   ii. The master of the ship should establish appropriate emergency response procedures for incidents aboard ship.

f. Harmonized plans – commercial waterfront facility and ship emergency response plans should be harmonized.

4. Security Training – The RSSI should verify with the commercial waterfront facility operator that all personnel involved in handling Class 1 materials are appropriately trained in security measures.

5. Spills – The RSSI should oversee clean up and repackaging of any spilled Class 1 materials.

6. Verifying quantities – The RSSI should verify that the quantities of Class 1 materials match the shipping papers.

7. Loading Ships
   a. Prior to loading, the RSSI should have a list of each carriers’ container(s) or trailer(s).
   b. The RSSI should confirm each container or trailer is on the list in section 3.5.7.1 above.
   c. Division 1.1, 1.2, and 1.3 materials should not be brought to the ship until it is ready to receive them.
   d. Loading of Division 1.1, 1.2, and 1.3 materials onto ships should proceed without unnecessary delay.

8. Unloading Ships
   a. Prior to unloading, the RSSI should have a list of each carriers’ container(s) or trailer(s).
   b. The RSSI should confirm each container or trailer is on the list in section 3.5.7.1 above.
   c. Division 1.1, 1.2, and 1.3 materials should not be unloaded from a ship until the means of further transport is ready to receive them.
   d. Unloading of Division 1.1, 1.2, and 1.3 materials from ships should proceed without unnecessary delay.
   e. When loading of vehicles and rail cars is completed, they should depart the berth as soon as practicable.
   f. The facility operator should conduct a visual inspection of the outside of packages or containers as they are unloaded from ships for unauthorized entry. Evidence of unauthorized entry or package tampering should be reported immediately to the RSSI and authorities.
   g. The consignee should be notified by the RSSI of any packages damaged or contaminated beyond repair or use. A determination of course of action should be
made at that time.

9. Loading and Unloading Motorized Vehicles
   a. Motorized vehicle drivers should remain in the immediate vicinity of their vehicles.
   b. Only the motorized vehicles needed to load, or unload Class 1 materials are permitted on the berth or inside the warehouse.

10. Attendance – Division 1.1, 1.2, and 1.3 materials in transit at the commercial waterfront facility should be guarded at all times.

11. Multiple Responsible Party Consultations - The handling of shipments of Division 1.1, 1.2, and 1.3 materials involving multiple shippers and/or consignees on or from ships should be planned in advance and coordinated by the facility operator to complete the process in the minimal amount of time while maintaining safety and security.

12. Communication - The RSSI should maintain communication with the U.S. Coast Guard, master of the ship, the facility operator, and the motor carrier, at all times when Class 1 materials are being handled.

13. Physical Security of Waterfront Facility
   a. The area at least 100 feet (30.5m) from where Division 1.1, 1.2, and 1.3 materials are handled should be restricted to only those individuals directly involved in the handling operation.
   b. The RSSI should maintain security by ensuring security plans are in place and adhered to.
   c. Only the minimum number of personnel needed to do the job safely and securely should be present at the berth when handling Class 1 materials.
   d. Waterfront facilities that handle Class 1 materials should meet the standard for interchange lots in the most recent edition of NFPA 498.

F. Rail – Rail is not generally used for transportation for commercial Class 1 materials. The handling of these rail shipments should be planned in advance and coordinated by the rail operator to complete the process in the minimal amount of time while maintaining safety and security.
SECTION IV – STORAGE

A. Site Control
1. Fences and Gates – Except where access is limited or controlled, ATF Type 1, 2, 4, or 5 magazine sites should be enclosed by fences with gates capable of being locked or electronically secured.
2. Entrances
   a. The number of entrances should be limited to the minimum number necessary to conduct operations.
   b. Entrance to the facility should be restricted and controlled to only those authorized to have access.
   c. Entrances should have a gate or other barrier that requires the vehicle to stop.
3. Firearms – Firearms should not be permitted on the facility without prior written authorization of the most senior person responsible for the operation of the facility (or the designee in the senior person’s absence), unless applicable law dictates otherwise.

B. Frequency of Inspection – Unless federal, state or local regulations mandate more frequent inspections, any person storing explosive materials should inspect magazines at least once every seven calendar days. However, more frequent inspections are recommended in person or by use of other surveillance technologies.

C. Magazines (vehicular, permanent, temporary)
1. Construction – magazines should be constructed in accordance with 27 CFR Part 555 Subpart K.
2. Limiting Storage Sites – the number of magazines and storage sites should be limited to the minimum number necessary to conduct operations and comply with quantity-distance standards or qualified quantitative risk assessments.
3. Inspections – The physical and functional integrity of magazines and the site should be inspected in detail at least monthly and any security issues addressed. The inspection should include but not be limited to the following items:
   a. Doors
   b. Gates and fences
   c. Vents
   d. Floors, foundations and skirting
   e. Roof
   f. Walls
   g. Lock hardware
4. Security Alarm System – If applicable, the security alarm system should be tested weekly to ensure it will operate as intended.

D. Vehicular Magazines (Bulk Trucks, semi-trailers, van trucks) – Preloaded vehicles that meet the requirements for and are used as a Type 5 magazine should be immobilized by one of the following methods:
1. Have wheels removed,
2. Be equipped with a kingpin locking device; or secure battery disconnect,
3. Be equipped with a steering wheel locking device and, if the magazine is unattended, secured by a fence and locked gate. Any person storing explosives materials in this manner should inspect such magazine at least once every 7 days, or
4. Bulk trucks used for storage must comply with the terms of the ATF Ruling, 2007-3.
E. Keys and Locks
1. Replacing Locks and Keys
   a. If explosives loss or theft occurs through non-forced entry in a magazine, the locks or lock inserts should be replaced on that magazine(s) and any others that use the same key set(s).
   b. If keys are lost, the associated locks or lock inserts should be replaced. A key should be considered lost if it is missing for 24 hours or more.
   c. If a terminated employee fails to return keys before leaving, the associated locks or lock inserts should be replaced immediately.
2. Key Access – The number of individuals that have access to keys should be restricted to the minimum number necessary to conduct operations.
3. Sign-in/sign-out Policy on Magazine Keys – Individuals should sign out and sign in magazine keys. Data such as the individual’s name, the date, time, and key number should be recorded.
4. Key Register – A record should be kept of key numbers, number of keys with that number, the number of locks keyed to that number, and their location.
5. Diversity of Locks and Keys – Separately-keyed locks should be used for gates and magazines.
6. Extra Lock – At least one extra lock with a unique key should be on hand should a replacement be needed.
7. Physical Security of Keys
   a. Keys should be kept in a secure lock-box.
   b. The key to the lock-box should be in the possession of the individual that maintains the key register.
8. Lock Standard – Padlocks should meet the “forcing” and “surreptitious entry” ratings of at least Grade 5 from the most recent version of ASTM F-883 and ATF standards.

F. Inventory recordkeeping
1. Frequency of inventory counts – Inventory should be reconciled at least quarterly.
2. Double counting – Product quantities should be counted at least twice upon receipt and shipment.
3. Verification of marks of identification – The manufacturer’s marks of identification should be visually verified and recorded when conducting unit counts.
4. Daily summary of magazine transactions – The daily summary of magazine transactions should include the manufacturer’s marks of identification.
5. Unit counts of open boxes – The number of units in open boxes should be recorded on the box and in the inventory.
6. Detonating cord inventory – The quantity of detonating cord in open boxes should be recorded by length.
7. Bulk explosives inventory - Bulk explosive and precursor materials (1.1, 1.2, 1.3 explosives & 5.1 oxidizers) should be handled in accordance with IME SLP-28.

G. Reporting Loss or Theft – Loss or theft of explosives must be reported in accordance with 27 CFR 555.30. Thefts of precursor chemicals should be reported to local authorities and to ATF.

H. Visibility or Clear Area
1. Around structures other than fences or gates – The land within 25 feet (7.6 m) of any magazine should be kept clear of rubbish, brush, dried grass, leaves, dead trees, all live tress less than 10 feet (3 m) high, and other combustible materials.
2. Around fences or gates – The land within 10 feet (3.05 m) of any fence or gate should be maintained for a clear field of view.
3. Large trees – To prevent access over the fence or gate, no large trees should be permitted.
I. **Access** – Access to ladders on bins or tanks containing 1.5 or 5.1 materials should be restricted by a locked ladder guard.

J. **Reconciliation** – Raw material usage should be reconciled with finished goods at least daily.

K. **Storage** – Each of the components of binary explosives should be stored in separate, locked containers.
SECTION V – USE

A. Blast Site Security
1. During the time that holes are loaded, or are being loaded with explosives, blasting agents, or detonators, the blast site should be barred to all but those authorized personnel engaged in the drilling and loading operations or otherwise authorized to enter the blast site.
2. The blast site should be attended, barricaded and posted, or flagged against unauthorized entry.

B. Blast Records – The blaster-in-charge (BIC) or their designee should complete an accurate blast record before leaving the blast site in every instance in which explosives are used.
1. Security Content of Blast Reports -- At a minimum, blast reports should contain the following security-related information:
   a. Local time of the blast accurate to the minute;
   b. Exact number and type of detonators used;
   c. Quantity and type of explosives used;
      i. Exact number and type of packaged products used, and
      ii. Quantity of bulk explosive used in pounds.
   d. List of names of all individuals present at the blast site during the loading operation including visitors.
   e. Notation of any unusual or suspicious activity.
2. Inventory Reconciliation
   a. The BIC should ensure that the amount(s) of explosive(s) reported used in the blast record plus the amount of explosive(s) returned to the magazine equals the quantity of explosives taken from the magazine.
   b. If partial case quantities of explosives are returned to the magazine, the number of remaining units should be displayed on the outside of the case.
   c. If bulk products are converted to packaged products at the blast site, special care should be taken to ensure that all packages are accounted for and used in the shot.

C. Conduct in Public – Blasting operations or techniques should not be discussed in public except in appropriate forums.

D. Attendance of Explosive Materials
1. Type 3 magazines containing explosives must be attended.
2. When outside of a locked magazine, explosives should be attended.
3. Explosives in an unlocked magazine should be attended.

E. Unused Explosives - All unused explosive materials must be returned to proper storage facilities as soon as possible and records updated.

F. Blasting Permits
1. If required, every person conducting an operation or activity requiring the use of explosive materials must:
   a. Obtain a permit to use explosive materials; and
   b. Allow the loading and firing to be performed or supervised only by a certified blaster.
2. Unless otherwise authorized, blasting permits should not be reassigned or transferred.
3. A blasting permit or a copy thereof should be posted at each place of operation.
4. Permit holders should take reasonable precaution to protect their permits from loss, theft, or unauthorized duplication, and any such occurrence must be reported immediately to the issuing authority.
G. Licensed or Certified Blaster

1. Licensed or certified blasters should carry a copy of their license or certificate on their person while handling or using explosive materials.

2. If the certification does not bear the blaster’s photograph, the blaster should carry government issued photo identification.

3. Blasters should take reasonable precautions to protect their licenses or certifications from loss, theft, or unauthorized duplication, and any such occurrence must be reported immediately to the issuing authority.
SECTION VI: SECURITY MEASURES DURING ELEVATED THREATS (AND DISASTERS)

Safety Library Publication (SLP) 27 is intended to offer security guidance to the explosives industry. During elevated threat levels or national emergencies, local, state, and federal agencies may provide additional mandatory instructions and/or other guidance.

The security measures in this section are recommended in addition to current regulatory requirements and should be considered for implementation when elevated threat levels are declared by DHS or otherwise deemed necessary. A full spectrum of threats must be considered (natural disasters, criminal and/or terrorist acts, civil unrest, accidental occurrences, etc.) on a location-by-location basis in order to understand the possible extent of damages and consequences and to enable the development of detailed action plans to address or mitigate each threat. These threats should be reviewed during normal security training (see Appendix E).

A. Perimeter Protection/Access Control
   1. Close and lock gates and barriers except those needed for immediate entry and egress.
   2. Control access to the facility with additional security personnel. Reduce facility access points to the absolute minimum necessary for continued operations.
   3. Keep all buildings and vehicles locked except when occupied.
   4. Monitor the perimeter of the facility with motion sensors, drones, cameras or guards. Increase security patrol activity.
   5. Ensure that barriers and other security systems are functioning and available for use. Adjust lighting to increase or decrease visibility.
   6. Limit visitors to the facility. Escort visitors while at the facility according to the site security plan.
   7. Prohibit unauthorized or unidentified vehicles/personnel entrance to the facility.
   8. Verify credentials of security personnel and law enforcement officials assisting with perimeter control.
   9. Inspect vehicles entering the facility, including cargo areas and undercarriage where dangerous items could be concealed.
   10. Restrict access to staging, shipping and receiving areas.
   11. Monitor restricted or critical areas (including power sources and storage tanks) within the facility with surveillance systems.
   12. Consider shutting down the facility and operations in accordance with security contingency plans.
   13. Implement business contingency and continuity plans as appropriate.

B. Communication
   1. Upon notification of a change in alert status and, at minimum, on a daily basis during elevated threats, ensure all means of communication, e.g. telephone, email, messaging, radio and satellite devices, electronic security systems, are in place and operational.
   2. Inform personnel of the change in alert status. Review with employees the operational plans, personnel safety, and security details and logistic requirements that pertain to the increased level as appropriate. Implement plans to provide periodic updates as well as the need to take additional security measures.
C. Manufacturing
1. Conduct a full inventory of explosives materials using at least two persons.
2. Resolve discrepancies immediately.
3. Reconcile raw material usage.
4. Increase frequency of full inventory counts.
5. Increase inspection frequency of magazine and bin storage.
6. Communicate results of reconciliations, inventories and inspections to appropriate personnel.

D. Sales and Distribution
1. Ensure that company “Know Your Customer” program is being followed, which may include a security review of new customers.
2. Confirm with ATF that new customers’ federal explosives license/permit is valid.
3. Consider using escorts or two drivers on vehicles transporting explosives.
4. Ensure a means of direct voice communication with drivers of vehicles carrying explosives.
5. Identify and plan for the use of acceptable safe havens on or near the designated route plan.
6. Ensure that vehicles transporting explosives are equipped with tracking equipment and that it is functioning properly.
7. Request for-hire carriers to provide information on the identities of drivers and vehicles prior to pick-up.
8. Advise customers of the products shipped, departure date and time, and estimated arrival date and time.
9. Expand route plan requirements for all explosives’ shipments; a copy must be retained by the shipper.
10. Require for-hire carriers and/or distributees (customers, recipients, etc.) to advise when deliveries arrive at their destination.
11. Ensure that all locks and seals on cargo compartments containing explosives are in place and working properly.

E. Use – Mining Quarrying and Construction
1. Double check blast record and quantities used
2. Ensure that BIC or their designee completes an accurate blast record prior to leaving the blast site
3. Attach copy of the drill log to the blast record
4. Double count all explosives taken from and returned to storage
5. Maintain a written list of all authorized persons permitted to be on the blast site

F. Oil and Gas Operations
1. Account for inventories of all moving explosives, including loaded perforating guns;
2. Confirm arrival of perforating guns at well sites;
3. Ensure loaded perforating guns are locked to racks, trucks or trailers to prevent unauthorized removal of the perforating guns or their explosives content; and
4. At continuously operating gun loading shops and well sites, ensure explosives security and accountability during shift changes, including:
   a. Conveying any security concerns noted on the previous shift to the incoming shift,
   b. Briefing to and/or verification by incoming shift of the quantities and types of explosives present,
   c. Reviewing any upcoming scheduled explosives deliveries to the site of operations or shipments from the site, and
d. Confirming any changes to personnel explosives access rosters.

G. Storage Sites and Portable Magazines on Job Sites
1. Consider expansion of patrolled area or addition of roving guards;
2. Assign personnel an area of responsibility for inventory and security.
3. Check magazines for evidence of tampering at least every twenty-four hours by varying the time and sequence or pattern of inspection;
4. Record time, date and results of magazine inspections;
5. Check magazines at job sites, including storage bins and drop trailers, at least daily;
6. Increase frequency of full inventory counts; and
7. Log trailers in and out when they enter and leave the site.
APPENDIX A – EXAMPLE FIXED SITE SECURITY PLAN

Note: The company and other names in this example are fictional and provided for educational purposes only.

Secure Explosives Company
Site Location, USA

Version: 1.0
Version Date: March 29, 2019

This plan is for the exclusive use of Secure Explosives Co. and its employees at the designated company site number. Employees may not distribute, release, or share information regarding this plan with any person outside the company, other than, as required by law and regulation, to duly authorized officers of a law enforcement or regulatory agency, without the express written consent of executive management.

Section I – Company Security Objectives
A. Respond to significant threats and vulnerabilities identified in the company’s risk assessment;
B. Assure that company personnel are vetted, including completion of background checks;
C. Provide training of employees in both general awareness of HazMat transportation security risks and company procedures;
D. Assure the safety and security of the company’s personnel, facilities, equipment, the cargo transported for our clients, and the general public with whom we come in contact;
E. Comply with federal, state, tribal and local laws and regulations;
F. Deter theft of company property and equipment and the cargo transported on behalf of our clients;
G. Respond to changes in the security environment according to the National Terrorism Advisory System (NTAS).

The contents of this security plan will be communicated to all company personnel and the designated site, according to their need to know, as illustrated in the table in the training section, except those portions of the plan which are denoted as being security sensitive information, which are accessible only to designated executives and the company’s security director.

Section II – Company Security Organization
Security is the responsibility of every employee of the company. Each employee has a responsibility to remain knowledgeable in and to comply with the company’s security policies and procedures, as applying to that particular employee’s position. All employees are responsible for reporting observations of breaches in security to their supervisors and, as their job duties require, to external authorities such as law enforcement agencies. All employees are encouraged to contribute suggestions which may improve the performance of this security plan to their supervisor or manager.

Management will actively monitor and test the performance of the security plan and will revise the plan as necessary to ensure that its objectives are met. The policies and procedures contained in this plan are effective as of the date shown above.
The following table describes the company’s security structure and the responsibilities of various personnel, by position or title, as appropriate.

<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibilities</th>
<th>Contacts</th>
<th>Crisis Team</th>
</tr>
</thead>
</table>
| Executive  | • Final approval of security plan and all revisions;  
• Approves changes in internal company threat alert levels;  
• Leads crisis team.                                                                                                                                                           | Barry Smart, Plant Manager  
(555) 555-2158 Work  
(555) 555-3147 Cell  
(555) 555-2925 Home                                                                                       | X                                                      |
| Security Director | • Prepares and maintains security plan  
• Prepares risk assessment and proposed changes to the security plan  
• Reviews all reports of security breaches  
• Maintains liaison with law enforcement and emergency response authorities  
• Monitors industry-wide intelligence information, alerts, and the national threat scenario  
• Ensures internal compliance with security plan and oversees verification  
• Implements and directs extra precautions for higher threat levels and in emergency situations  
• Maintains all security sensitive information in a secure manner;  
• Ensures compliance by human resources of personnel security provisions                                                                                           | Same as above                                                                                     | X                                                      |
<table>
<thead>
<tr>
<th>Position</th>
<th>Responsibilities</th>
<th>Contacts</th>
<th>Crisis Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manager</td>
<td>• Supervises implementation of security plan at facility</td>
<td>Getsit Dunn, Production Supervisor (555) 555-2213 Work (555) 555-3144 Cell</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Monitors employee performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reviews and reports security breaches to security director, law enforcement and intelligence channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ensures that human resources files are properly documented and updated</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ensures that company records and communications are appropriately secured</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitors all fleet movements for compliance with company routing and communication requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production Technicians</td>
<td>• Complies with all company requirements for secure loading and transport of shipments</td>
<td>Maintained by human resources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Inspects vehicles for evidence of tampering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Maintains vigilant observation for unusual or suspicious behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monitors all facility and perimeter security and persons accessing facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Detains and questions unauthorized persons if reasonably possible</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Reports emergency security breaches to law enforcement and reports all security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab/Office</td>
<td>• Maintains alert observations and reports security discrepancies to manager</td>
<td>Maintained by human resources</td>
<td></td>
</tr>
</tbody>
</table>
Section III – Risk Assessment
The company has carefully assessed the potential vulnerabilities of its facility and operations in light of the current general terrorism threat situation, the nature of the operations, the location of our facilities, and regulatory requirements.

The company has determined that potentially significant security threats exist with certain operations. For purposes of designation and applying its security policies and identifying potentially vulnerable operations, a general assessment will be communicated to employees, as appropriate to their duties. (For additional guidance on conducting a risk assessment, see Appendix F.)

Section IV – Security Procedures
Examples of Security Policies in a Three-Tiered Company Alert System

The company has determined to model its alert system after that of the U.S. Department of Homeland Security NTAS using, however, only three levels of alert instead of five. The company will actively review its alert status whenever the NTAS Alert condition is changed.

A Normal Situation will be the baseline condition for all company operations and facilities and will be the default for normal conditions. Under NTAS Elevated Alert, the company will immediately go to an Elevated Threat Situation if the threat alert affects its operations or Level 1 and 2 materials. Otherwise the security director, with approval of the Executive, will review available information and declare the proper security situation. When NTAS Imminent Alert is declared, it is presumed that it will be selectively applied. Any company operation affected by the NTAS Imminent Alert will immediately go to Extreme Threat Situation alert level, and the security director, with approval of the executive, will review available information and declare the proper security situation.

<table>
<thead>
<tr>
<th>Security Activity</th>
<th>Normal Situation (No NTAS Alert)</th>
<th>Elevated Situation (NTAS Elevated Alert)-Additional Procedures</th>
<th>Imminent Situation (NTAS Imminent Alert)-Additional Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel Procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to Facilities and Operations Areas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loading/ Unloading</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HazMat Storage and Holding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records and Cyber</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section V – Records Security
The master copy of the security plan will be maintained by the Security Director. All copies of the complete security plan are considered restricted security sensitive information (SSI), as are any communications from government agencies bearing the SSI designation, and will be made available only to designated company personnel and appropriate regulators. All SSI designated materials will be maintained in a locked file cabinet accessible only to the Security Director. Facility and operations managers will have access to the risk assessment for the facility.

All customer information, security reports, and the like are restricted to those whose job responsibilities are need-to-know for that information. Employees will be issued individual IDs and passwords for computer stored records by the computer department manager, which may not be shared with any other individual. Personnel records may only be accessed by the human resources department and the employees.

Section VI – Communications
All necessary company vehicles and equipment will have the ability to communicate remotely. The company provides one or more operating two-way radios or cell phones. Communication requirements are set forth in the company policies throughout this plan. It is the responsibility of every employee to know, understand and comply with communications requirements applicable to their job duties.

Section VII – Breaches in Security
All significant security breaches which pose an apparent imminent danger to the company, its employees, equipment, facilities or cargo will be reported to law enforcement immediately, and to the Manager. All other significant breaches in security will be reported to the manager and to the Security Director, who will determine the proper handling.

All non-significant security breaches will be reported to the Manager, who will respond according to the nature of the event and maintain records of the events. All event logs will be submitted to the Security Director for review monthly.

A significant security breach can be:
A. Any actual attack or apparent attack
B. Any incident involving actual or attempted hijacking
C. Any deliberate act aimed at stopping a vehicle or intended to cause an accident
D. Any incident involving the use or threatened use of weapons of any kind
E. Any discovery of sabotage or attempted sabotage of any shipment, equipment or security system
F. Any attempt or apparent attempt to ship illicit weapons through the company’s services
G. Any unexplainable failure of security technology and systems
H. Unauthorized non-company personnel found in or attempting to enter areas involving Level 1 and 2 HazMat operations, tank trailers and other specialized equipment for transporting Level 1 or 2 materials
I. Any loss, theft or compromise of security sensitive information
J. Any cyber-attack against the company’s business systems
K. Employees accessing or attempting to access information or areas for which they are not authorized
L. All other violations of company security policies and procedures
M. Observations of apparent or suspected characteristic terrorist operational acts
Section VIII – Training
All company employees will receive awareness training in general recognition, awareness, and reporting terrorist behavior and reporting of suspicious behavior and incidents. Awareness training is summarized in an employee handout. In addition, every employee will be trained in the security policies and procedures of this plan as relevant to each employee’s job function. This training will be conducted within 90 days of employment in a HazMat position and every three years thereafter; training will also be conducted within 90 days of revision of this security plan.

Section IX – Verification
The company will schedule verification drills and inspections to ensure compliance with this security program on a random basis, at least once per year at each facility. Managers will conduct observation and periodic systems testing at random intervals throughout the year. More frequent verifications will be conducted in facilities and operations which consistently show deficiencies. Observations will be recorded as appropriate and maintained as Restricted Access by both the Manager and Security Director.

Section X – Review and Revisions to the Plan
The company will review the security records and performance of all operations at least once per year to determine if any revisions are needed to this plan. For each significant breach of security, the security director will determine whether any interim modifications are required. Revisions are effective after approval by the Executive and the Security Director. Copies of the plan or portions thereof, as applicable to various operations and employees’ need-to-know, will be circulated to be available on the effective date. Copies of the plan at the corporate and facility offices must display complete approvals.

Section XI – Approvals

Plan Edition: __________________________

Effective Date: ________________________

Executive/Security Director: __________________________

Name Date

Manager: __________________________

Name Date
APPENDIX B – RECOMMENDED ELEMENTS OF A TRANSPORTATION SECURITY PLAN

The purpose of a Hazardous Materials Transportation Security Plan is to establish companywide policies, procedures, and guidelines to mitigate risk during road transportation operations. The plan must comply with Federal Motor Carrier Safety Administration (FMCSA) and Research and the Pipeline and Hazardous Materials Safety Administration (PHMSA) regulations for “offerors and transporters” of hazardous materials.

The items contained in this section are general topics that should be considered for inclusion in company transportation security plans. The topics, as described, are not comprehensive, nor are they intended to cover every security situation that could potentially be encountered during transportation. An in-depth Example Transportation Security Plan, utilizing these topics, can be viewed at www.IME.org. Additional information regarding the transportation of explosives can be found in IME SLP-14, Handbook for the Transportation and Distribution of Explosive Materials.

A. Scope
This section should describe in detail the Hazmat carrier’s operation including the type of power units and containers utilized during transport and incidental storage.

B. Key Aspects of the FMCSA/PHMSA Regulation
This section should describe pertinent elements of FMCSA/PHMSA regulations. The regulations require that operators perform an assessment of the transportation security risks associated with the materials they handle, and that each plan be based on a company's assessment of the security risks associated with the materials it ships or transports.

C. Overview of Transporter's Hazmat Operations
This section should include procedures for verification of drivers’ credentials and identify driver screening methods used. Methods used to communicate with drivers and company policies relative to security within terminals should also be included.

D. Risk Assessment
This section should describe risk assessment requirements and methodology(ies) used by the company. A risk assessment should identify potential risks during transport and should be used to develop policies and procedures to counteract or reduce the identified risk.

E. Roles and Responsibilities
This section should describe internal company committees and identify individuals responsible for implementing and managing the Hazmat security plan and program.

1. Corporate Security Committee
   A corporate security committee should be established to provide oversight of the carrier’s Hazmat security program and ensure that appropriate and uniform guidelines are established and implemented.

2. Field Managers
   The company should designate Field Managers responsible for implementing the corporate policies and security protocols at individual locations. The company should develop a clear reporting structure throughout the carrier’s chain of command to be used in reporting security incidents.

3. Hazmat Personnel
   The company should establish hazmat personnel responsible for learning and applying security policies and procedures.

F. Job Applicant Background Investigation
This section should describe company requirements and procedures regarding employee background investigations. A background investigation is essential to a hazmat carrier’s evaluation of potential employees.

G. Hazmat Access Controls and Procedures
The transportation security plan should address the company’s procedures for controlling access to
security sensitive transportation areas. At a minimum, this section should cover access to the carrier’s power units and in-transit approved parking areas. The implemented controls and procedures should prevent unauthorized access to the power unit or cargo compartments and prevent unauthorized access to restricted parking areas.

H. En Route Security

The security of hazmat during transport is dependent upon the vigilance and security practices of the carrier’s drivers. The company security plan should discuss the carrier’s established policies regarding route security and emphasize the importance of adhering to such policies. Policies should include security procedures for stopping at facilities, such as fueling areas, and route schedule compliance monitoring and reporting. A discussion of carrier-provided communication and tracking systems should also be included in this section of the plan.

I. Security Measures for Elevated NTAS Threat Levels

The plan should outline the company’s response(s) to changing NTAS Threat Levels. When Department of Homeland Security (DHS), National Terrorism Advisory System (NTAS) elevates the nation's threat level, implementation of additional security measures should be considered for hazmat operations. Security measures in response to elevated threat levels should be appropriate and customized to the specificity of the threat and the potential impact of the threat to the road transportation of hazardous materials.

J. Security Incidents – Response and Reporting

This section of the plan should describe how the company will handle security incidents. Security incidents in hazmat operations can take many forms, range widely in degree of severity, and require various responses. The safety of hazmat personnel, contractors, visitors, and the general public is of paramount importance during security incidents, and all response and reporting procedures should reflect that goal.

K. Reporting Threat Information

The company policy should include procedures for reporting threat information. As with security incidents, the safety of hazmat personnel, contractors, visitors, and the general public is of paramount importance. All threat reporting policies and procedures should reflect that goal.

L. Communications with Law Enforcement

The policy should include a section on how the company will conduct communications with law enforcement. It is essential that open lines of communication be maintained with law enforcement officials at the local, state, and federal levels. Not only are law enforcement officials’ reliable sources of threat information and security guidance, they also serve as first responders to security incidents.

M. Employee Training and Security Awareness

This section of the plan should describe the company’s program(s) for training employees in security awareness. The employee security awareness training program should focus on topics such as hazmat security plan, FMCSA regulations, threats, procedures, policies background investigations and roles and responsibilities.

N. Internal Security Audit and Verification Program

Security audit and verification program(s) should be described in this section of the plan. The carrier should implement a yearly internal audit of transportation-related security practices to ensure appropriate measures are in place.
APPENDIX C – SAMPLE QUESTIONS WHEN ASSESSING YOUR VULNERABILITY

Are your explosives available for misuse?
It is essential for all persons involved with explosives and explosives related activities to maintain effective control of explosive materials. To this end the following question are suggested to help determine if control is being maintained.

A. OVERALL OPERATIONS MANAGEMENT
   Who is responsible for ensuring adherence to the explosives operating procedures?

B. EXPLOSIVES ACCESS
   Who has access to your explosives? Why?
   Who knows about your explosives? Why?
   Who has access to keys? Why?
   Where are keys kept? Secure?
   Are there spare keys? Where? Secure?
   Are the people with access to explosives authorized and appropriate people?
   Would you know if some of your explosives went missing? How?
   Who is responsible for controlling access to explosives?

C. EXPLOSIVES MAGAZINES
   Are magazines properly and appropriately secured? Meet standards?
   Are magazines located in a secure location?
   Who has keys? Secure?
   Who has access to the magazines? Why?
   Is there a responsible person assigned? Is the person appropriate?
   Are magazine records checked regularly for accuracy? Inventories?
   Have discrepancies been detected? How?
   Who investigates discrepancies? Report to whom?
   Are magazines locked at all times, except during the loading and/or unloading process?
   Is separate storage provided for detonators? Secure?

D. MAGAZINE KEEPER
   Is there only one keeper? If not, Why?
   Is the keeper an appropriate/competent person?
   Who is responsible for monitoring the activities of the magazine keeper?

E. TRANSPORT OF EXPLOSIVES
   Are transporter credentials verified prior to each shipment?
   Are explosives transported in locked containers, bins and IME 22 boxes? Why not?
   Where are keys kept? Spares? Secure?
   Are the explosives constantly attended? Why not? If not, are they secure?
   Are explosives segregated from detonators?
   Are drivers of vehicles trained, competent and appropriate for their jobs?
Are drivers capable of communicating with the company and vice versa? Why?

F. USE OF EXPLOSIVES
Is access to explosives controlled during use?
Are unused explosives returned to the magazine when it is determined that they are no longer needed at the point of use? Why not?
Are all persons trained and competent for the work involved? How do you know?
Are persons appropriately vetted for the work involved?
Are all explosives accounted for at the point of use? How?
Are all explosive materials carefully monitored, particularly detonators? How?
Would a discrepancy be detected? How? When?
Are discrepancies recorded? Investigated? Reported to whom?
Are any blasts audited for explosives use vs. design? Are explosives on site constantly attended? Secured?
Who is responsible for monitoring explosives at the work site?

G. MANUFACTURE OF EXPLOSIVES
Are only authorized personnel allowed access to explosives and precursors (all explosive components and ingredients)?
Are records of all explosive material maintained? How?
Are persons involved trained, competent and appropriate? Why?
Would discrepancies in inventory of explosives or explosive components be detected? How? Investigated?
Are always explosives monitored /secured when outside magazines? Are random searches conducted of people and vehicles? Why not?
Who is responsible for monitoring explosives in the manufacturing environment?
Are scrap explosive materials properly accounted for and disposed?

H. SALE AND PURCHASE OF EXPLOSIVES
Are persons who sell and purchase explosives trained, responsible and appropriately vetted? How do you know?
Are sales and purchases only made to and by authorized persons? How do you know?
Are licenses or permits checked and confirmed to be valid prior to sale?
Are transporter credentials verified prior to each shipment?
Are detailed sale or transaction records maintained? Where? Are these checked?
Are explosives stocks or inventory recorded, checked, reconciled? By whom?
Are explosives secured at all times? If not, why?
Are discrepancies investigated? By whom? Report to whom?

I. DISPOSAL OF EXPLOSIVES
Who is responsible for proper disposal of explosives and explosive components?
Are explosives awaiting disposal properly stored in magazines?
Are detailed records of explosives disposal maintained?
Where? Are checks carried out to ensure explosives are destroyed? How? Are any random searches carried out on persons and vehicles? Why not?

J. SUSPICIOUS ACTIVITIES
Can your employees identify suspicious activities? Is awareness training necessary? (“When in Doubt Point It Out” TM posters are available from IME).
Do employees know to whom to report suspicious activities? Site Manager? Local police? ATF?
Controlling access to the plant, explosives and facilities is of utmost importance. The method for controlling access by personnel should be customized to the company’s security profile. Visual identification should be distinct for each level of access, as illustrated by the examples below:

**GREEN** (Level 1) – unlimited access to all areas

**YELLOW** (Level 2) – limited access without direct supervision

**RED** (Level 3) – escort required at all times, in all areas

**Examples:**

- Jane Doe
  - Safety Manager
  - Full access to all areas

- Jane Doe
  - Production
  - Escort required

- Jane Doe
  - Administration
  - Turnstile access only
APPENDIX E – CYBER SECURITY MEASURES

While physical security is paramount to industry security, cyber security also plays a major role in protection of facilities and operations. As technology that affects cyber security advances, the need for robust security measures becomes increasingly important. While it may be impossible to combat all cyber threats, a proactive defense is the most effective way to minimize the potential impact of malicious actors. The following steps should be considered in developing and maintaining effective cyber security.

Base Line Analysis
The following steps should be taken when creating a cyber security plan. The plan should be reviewed when there are operational changes, as new potential threats are identified, and/or at least annually.

A. Analyze potential threats (who could they come from and what would they want?)
B. Analyze vulnerabilities (what tactics could be employed to gain access to systems and information?)
C. Assess risk (what measures have already been instituted to mitigate risk and the time/resources required to fill in any security gaps?)

Facility and Operation Cyber Security Measures
The following measures should be instituted to prevent loss of information and systems control.

A. Limit internet access for confidential data/processes/controls.
B. Verify network security features are current on all devices (update phone software as soon as possible and update computer security software automatically).
C. Limit data management authority to employees whose job responsibilities require access.
D. Verify data storage (if offsite, verify source quality and security standards, and if in the cloud, secure with password).
E. Create discretionary access controls (specific data accessible for a specific period).
F. Create a secure remote access Virtual Private Network (VPN) if offsite cyber access is required by employees.
G. Create a system-wide “breach in security” alert.
H. Establish a location specific Cyber Security Policy tailored to individual facility needs.
I. Develop capability to detect wireless and remote intrusion and surveillance attempts.

Control Systems
Network based control systems should include all critical components to the location specific operation. These controls should prevent unauthorized access to the control systems and prohibit the ability to override any intended process.

Individual Considerations
The following are measures individuals can employ to protect themselves and the workplace:

A. Do not run email or accounting programs on point-of-sale software (commonly used in retail transactions).
B. Verify the legitimacy of email attachments and links, even from known sources.
C. While working offsite, verify internet connection via individually unique password on public networks, utilize VPN, and/or use personal hotspot for enhanced security.
D. Verify that operational patches to software programs do not damage security protocols on devices.
E. Do not give administrative access to third party systems/programs.
F. Enable password reset notifications which can indicate attempted unauthorized access.
G. Do not use the same passwords for different accounts and change passwords every 90 days.
H. Do not record passwords unless stored in a reputable and secure password management program.
For more information on Cyber Security, please visit: http://csrc.nist.gov/publications/PubsSPs.html and https://www.dhs.gov/cisa/rbps-8-cyber.
APPENDIX F – TRAINING

The security training of employees working with or overseeing operations involving the manufacture, purchase, sale, transportation, storage and use of explosives and precursor chemicals is integral to the success of any security plan. This should include both initial and recurrent security training.

Elements of Security Training Plans
In-depth security training involving specific security procedures and the duties and responsibilities of each employee must be in every security plan. Training should encompass general recognition, awareness, and reporting of behavior and incidents that is suspicious or has the marking of terrorist or criminal behavior. Training plans should involve a clear and comprehensive review of company security objectives, the organizational security structure along with a review of the assessed security risks.

Review of Security Training Plans
Security training plans should be reviewed at least annually to determine the effectiveness of the training materials. Changes and communications related to the security training plan need to be fully documented. When it is necessary to amend the security plan, an assessment should be completed to determine which employees require retraining and which employees simply require notification of the changes.

Frequency of Security Training
- Each employee engaged in explosives operations must receive security training prior to being permitted access to any explosive’s records, storage, or operations, including any changes of assignment, responsibility or facility.
- Reviewing security training (refresher training) is essential to ensure that those who have security duties and responsibilities know what is expected of them. The interval of time between such refresher training should not exceed one year.
- Training on revised security plans should be conducted within 90 days of the plan revision, however, training for substantial and significant changes to the security plan should be conducted immediately.

Documentation of Training
Documentation of security training should reflect the names of personnel who received training, sufficient information regarding curriculum that was delivered and how it was delivered (e.g. in-person, web conference, or electronic), and the date of training delivery. Training records should be completed within 90 days of completion of the training course and records should be maintained for a minimum of three years or at least 90 days following the date of any employee’s departure.

Outside Service Providers
Refer to corporate policies where outside service providers need to be apprised of the changes to policies or procedures.
APPENDIX G – RISK ASSESSMENT

Formal Risk Assessment
The company’s risk assessment is considered security sensitive information and will be restricted to a limited, authorized distribution list on a need to know basis.

Risk assessments should be conducted throughout all aspects of manufacturing, transportation, storage and use of commercial explosives. Each position of the explosive and precursor materials throughout these processes offer unique risks and may require different procedures to minimize risk.

Companies should design and deploy countermeasures, procedures, and systems in order to avoid, reduce or mitigate the risk presented by various scenarios. Decision making should be based upon its evaluation of the effectiveness of its programs, as illustrated by the example below.

Example:
The company has determined that its operations and facilities have a potential risk of attack or exposure to the following scenarios: theft of equipment and material, hijacking and sabotage.

The company’s risk assessment evaluated exposures for Level 1 and 2 materials in relation to the following potential attack scenarios. It has determined and classified the relative risks posed in light of identified vulnerabilities and threats and assigned a relative score.

- Scores were given on a scale ranging from zero to five with scores of five indicating the highest consequences or easiest acts.
- Level 1 Materials - These materials present a significant security risk. Example: All explosive and precursor materials
- Level 2 Materials - These materials present a minimal security risk. Examples: gasoline, diesel fuel

Each scenario with a score of 225 or less will be addressed in the company’s Normal Situation security procedures. Scenarios with a score of 226 to 400 will be addressed in the company’s Elevated Threat Situation security procedures. Scenarios with a score of 401 to 625 or greater will be addressed in the company’s Imminent Threat Situation security procedures. This analysis can also identify areas of excessive vulnerability that warrant corrective action.

<table>
<thead>
<tr>
<th>Threat</th>
<th>L</th>
<th>W</th>
<th>D</th>
<th>T</th>
<th>C</th>
<th>CF</th>
<th>V</th>
<th>A</th>
<th>E</th>
<th>R</th>
<th>S</th>
<th>FF</th>
<th>TPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>20</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>14</td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hijack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Attack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

35
<table>
<thead>
<tr>
<th>Consequences</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• L-potential for loss of life</td>
<td>• V-how easy for an unauthorized person to discover</td>
</tr>
<tr>
<td>• W-use/convertibility to a weapon</td>
<td>• A-how easy for an unauthorized person to gain access?</td>
</tr>
<tr>
<td>• D-physical damage potential</td>
<td>• E-how difficult is the scenario?</td>
</tr>
<tr>
<td>• T-political/economic target value</td>
<td>• R-can the acts be easily rehearsed?</td>
</tr>
<tr>
<td>• C-collateral, consequential and economic damage potential</td>
<td>• S-amount of required resources</td>
</tr>
<tr>
<td>• CF- consequential factor = L+W+D+T+C</td>
<td>• FF-feasibility Factor= V+A+E+R+S</td>
</tr>
<tr>
<td></td>
<td>• TPS=threat potential score=CFxFF</td>
</tr>
<tr>
<td><strong>SLP Number</strong></td>
<td><strong>SLP Title</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SLP – 1</td>
<td>Construction Guide for Storage Magazines</td>
</tr>
<tr>
<td>SLP – 2</td>
<td>American Table of Distances</td>
</tr>
<tr>
<td>SLP – 3</td>
<td>Suggested Code of Regulations for the Manufacture, Transportation, Storage,</td>
</tr>
<tr>
<td></td>
<td>Sale, Possession and Use of Explosive Materials</td>
</tr>
<tr>
<td>SLP – 4</td>
<td>Warning and Instructions for Consumers in Transporting, Storing, Handling</td>
</tr>
<tr>
<td></td>
<td>and Using Explosive Materials</td>
</tr>
<tr>
<td>SLP – 12</td>
<td>Glossary of Commercial Explosives Industry Terms</td>
</tr>
<tr>
<td>SLP – 14</td>
<td>Handbook for the Transportation and Distribution of Explosive Materials</td>
</tr>
<tr>
<td></td>
<td>Use of Commercial Electric Detonators (Blasting Caps)</td>
</tr>
<tr>
<td>SLP – 22</td>
<td>Recommendations for the Safe Transportation of Detonators in a Vehicle with</td>
</tr>
<tr>
<td></td>
<td>Certain Other Explosive Materials</td>
</tr>
<tr>
<td>SLP – 23</td>
<td>Recommendations for the Transportation of Explosives, Division 1.5,</td>
</tr>
<tr>
<td></td>
<td>Ammonium Nitrate Emulsions, Division 5.1, Combustible Liquids, Class 3, and</td>
</tr>
<tr>
<td></td>
<td>Corrosives, Class 8 in Bulk Packaging</td>
</tr>
<tr>
<td>SLP – 24</td>
<td>Recommendations for Handling 50 Metric Tons or more of Commercial Division 1.1</td>
</tr>
<tr>
<td></td>
<td>or 1.2 Break-Bulk and Containerized Explosive Materials in Transportation at</td>
</tr>
<tr>
<td></td>
<td>Commercial Waterfront Facilities in the United States</td>
</tr>
<tr>
<td>SLP – 25</td>
<td>Explosives Manufacturing &amp; Processing Guideline to Safety Training</td>
</tr>
<tr>
<td>SLP – 27</td>
<td>Security in Manufacturing, Transportation, Storage and Use of Commercial</td>
</tr>
<tr>
<td></td>
<td>Explosives</td>
</tr>
<tr>
<td>SLP – 28</td>
<td>Recommendations for Accountability and Security of Bulk Explosives and Bulk</td>
</tr>
<tr>
<td></td>
<td>Security Sensitive Materials</td>
</tr>
<tr>
<td>SLP – 30</td>
<td>Safe Handling of Solid Ammonium Nitrate</td>
</tr>
<tr>
<td>SLP – 31</td>
<td>Methods and Algorithms Used for Quantitative Risk Analysis</td>
</tr>
<tr>
<td>SLP – 32</td>
<td>Recommendations for Safe and Secure Use, Storage, and Transportation of</td>
</tr>
<tr>
<td></td>
<td>Commercial Explosives in Oil and Gas Operations</td>
</tr>
</tbody>
</table>
What is IMESAFR?

Institute of Makers of Explosives (IME) Safety Analysis for Risk (IMESAFR) is a software model that was developed through a joint effort by IME and A-P-T Research, Inc.

IMESAFR is a probabilistic risk assessment tool used to calculate risk to personnel from explosives facilities. This software not only calculates Quantity Distances (QD) based on the American Table of Distances and other QD regulations, it can determine a level of safety based upon risk.

IMESAFR uses the donor structure and activity, the structure of the exposed sites, and duration of exposed personnel to determine a level of safety. The program provides users with the ability to work in metric or imperial measures, and allows users to import maps or drawings of their site to assist with visualizing facility layouts and results.

Why was IMESAFR developed?

IMESAFR was developed to provide a more comprehensive assessment of the overall risk of explosives operations. The commercial explosives industry in the United States uses the American Table of Distances (ATD) as the basis for safe siting of explosives storage facilities. ATD siting involves the evaluation of a specific magazine and inhabited building or public highway, which are referred to as a Potential Explosion Site (PES)/Exposed Site (ES) pair in IMESAFR. This evaluation yields the recommended separation distance based on the factors that affect risk, including whether a barricade exists. Although the same criteria can be applied to explosives manufacturing operations, the ATD was intended for use in limited permanent storage situations. In addition to permanent storage situations, IMESAFR accounts for other activities such as manufacturing, assembly, and loading and unloading.
IMESAFR Training Course

The course is presented over three days with eight hours of mixed lecture and discussion each day for a total of 24 classroom hours. Daily class hours are from 8am to 5pm with an hour for lunch and breaks mid-morning and mid-afternoon. A competency test will be given at the end of the course.

Class Size: minimum of 10, maximum of 25.

Where
The class is normally held at the APT Safety Engineering and Analysis Center (SEAC) in Huntsville, AL, conveniently located in Cummings’ Research Park near Redstone Arsenal.
See www.apt-research.com/contacts/contactUs.html for detailed directions.

The class may also be offered at other locations. On-site training courses can be arranged, as well as courses that run in conjunction with conferences and meetings.

Course Content
The IMESAFR Training Course will guide the user through the overall user interface of the IMESAFR Software. Some of the topics discussed are listed below.

- A background on the concepts and terminology used in the IMESAFR risk assessment software.
- A thorough guide on using input screens and choosing the proper input selection.
- A description of the capabilities of IMESAFR including menu options, functions of the tool bar, help menu and generating reports.
- An overview of the 26-step process used by IMESAFR to familiarize the user with the exposure and consequence analysis.
- Multiple examples (some worked individually and some as a group) demonstrating the various capabilities of IMESAFR.
- Practical applications of the software and its use in the risk management process.

Course Outline
1. Overview
2. QD Concepts & Background
3. QRA Concepts & Background
4. IMESAFR Features
5. Class Exercise 1
6. Risk Management
7. Advanced Tools
8. Architecture - Part 1
9. Architecture - Part 2
10. IMESAFR Protocols
11. Linking Architecture to Testing
12. Class Exercise 2
13. Approval Process
14. Input Decisions
15. Group Exercise
16. Test

Each student is responsible for bringing a laptop to training. A training book is included in the course fee.

Schedule
apt-research.com/training

CEU
Upon completion of this course, attendees will be credited with 2.0 Continuing Education Units (CEU).

Cost
IMESAFR v2.1 Training: US$1800
IMESAFR v2.1 Software:
- Standard Price: US$1500
- IME member: US$750
Upgrade software from v1.x to v2.1:
- Non IME member: US$750
- IME member: US$375

Registration Information
To register for a class in Huntsville or if you are interested in setting up a training course at a location other than Huntsville, please contact:
Mary Robinson, 256.327.3373
imesafatraining@apt-research.com

It is the policy of A-P-T Research, Inc., that those leading a learning event (instructors, guest lectures, etc.) disclose proprietary interest in any products, services, instruments, devices or materials discussed during a learning event. This includes any source of third-party compensation. Leaders of a learning event are required to disclose this information in the form of a verbal announcement at the beginning of the learning event.
When in doubt, put it out™

REPORT SUSPICIOUS ACTIVITY

Contact the site manager: Insert Phone Number

Site Manager – Contact local law enforcement and/or ATF at (800) 800-3855

International Society of Explosives Engineers

Institute of Makers of Explosives
DESTRUCTION OF COMMERCIAL EXPLOSIVE MATERIALS

At times it may be necessary to destroy commercial explosive materials. These may consist of explosives or blasting agents from containers that have been broken during transportation or may be materials that have exceeded their recommended shelf life or are believed to be overage or are no longer needed.

Due to the many developments in explosive technology over the past few years, the appearance and characteristics of products have undergone marked changes. To be sure that you are familiar with the properties of the product that you plan to destroy, the manufacturer of that product should be consulted for the most current product information and the recommended method of disposal and/or destruction.

The member companies of the Institute of Makers of Explosives have agreed to supply advice and assistance in destroying explosives. If the manufacturer is known, seek his assistance. If the manufacturer is not known, a member company of the Institute of Makers of Explosives may provide advice or assistance.

The above policy of IME member companies relates only to commercial explosive materials. It does not include handling improvised explosive devices or bombs, military ordnance, military explosives, or homemade explosive materials.

IME member companies also cannot become involved in destroying explosive materials, which have been used for illegal purposes, are reportedly stolen property or are considered as evidence in any potential civil litigation or criminal prosecution.
IME
institute of makers of explosives

BLASTING CAPS ARE DANGEROUS EXPLOSIVES
IF YOU FIND ANYTHING THAT LOOKS LIKE THIS REPORT IT PROMPTLY TO THE NEAREST POLICE OR FIRE DEPARTMENT

ime.org
info@ime.org

Printed in the USA