

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

This document contains a description of the voluntary security practices (referred to as Security Action Items or SAIs) that the Transportation Security Administration (TSA) is recommending to increase the security of certain highway security-sensitive materials transported by motor vehicle. TSA intends that this document be used along with the listing of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) or Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM) (Appendix B) and the Security Assessment conducted to satisfy Pipeline and Hazardous Materials Safety Administration (PHMSA) requirements under 49 CFR 172.802 to determine the appropriate voluntary security practices to be implemented for the indicated substances when transported in the volumes noted in Appendix B. The listing of Tier 1 and Tier 2 HSSM provided in Appendix B is not intended to meet the requirements to develop a list of security sensitive materials as defined in section 1501 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

The voluntary security practices have been developed by TSA Office of Transportation Sector Network Management, Highway and Motor Carrier Division after consultation with individual stakeholders including chemical manufacturers, chemical carriers and transportation industry representatives, as well as appropriate Federal agencies. TSA will consider revisions to the SAIs based on experience in the implementation of the SAIs and the suggestions of stakeholders and Federal agencies.

The recommendations in this document are not intended to conflict with or supersede any existing regulatory or statutory requirements. In the case of conflicts, TSA encourages stakeholders to implement non-conflicting recommended security actions.

The following definitions are applicable to this document:

Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. For purposes of these SAIs, Critical Infrastructure refers to those portions of all Federal, State, and local highway systems that, as a result of a terrorist activity, could reasonably be expected to be time consuming, disruptive to the regional economy and costly to replace. This may include publicly and privately owned infrastructure that is deemed critical by Federal, State, local or tribal governments.

Hazardous Materials – means “hazardous material” as defined by the U. S. Department of Transportation in 49 CFR 171.8.

Hazmat – means a hazardous material.

Highway Transportation Sector Hazmat Employee (employee) – means:

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

(1) A person who is employed on a full time, part time, or temporary basis by a highway transportation sector hazmat employer and who in the course of employment directly affects transportation security of HSSM;

(2) A person who is self-employed (including an owner-operator of a motor vehicle) transporting hazardous materials in commerce who in the course of such self-employment directly affects transportation security of HSSM;

(3) This term includes an individual, including a self-employed individual, employed by a motor vehicle hazmat employer who, during the course of employment:

- (i) Loads, unloads, or handles HSSM;
- (ii) Prepares HSSM for transportation;
- (iii) Is responsible for the security of transporting HSSM; or
- (iv) Operates a vehicle used to transport HSSM.

Highway Transportation Sector Hazmat Employer (employer) – means:

(1) A person who employs or uses at least one hazmat employee on a full time, part time, or temporary basis; and who:

- (i) transports HSSM in commerce; or
- (ii) Causes HSSM to be transported in commerce;

(2) A person who is self-employed (including an owner-operator of a motor vehicle) transporting HSSM in commerce and in the course of such self-employment directly affects the transportation security of HSSM.

Highway Security-Sensitive Materials (HSSM) – a material identified by TSA as posing a significant risk to national security while being transported in commerce due to the potential use of the material in an act of terrorism. A HSSM may, at a minimum, include the following material as defined in 49 CFR 171.8:

- (A) Class 7 radioactive materials.
- (B) Division 1.1, 1.2, or 1.3 explosives.
- (C) Materials poisonous or toxic by inhalation, including Division 2.3 gases and Division 6.1 materials

Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) – HSSM transported by motor vehicle whose potential consequences from an act of terrorism include a highly significant level of adverse effects on human life, environmental damage, transportation system disruption, or economic disruption. Attachment B contains a listing of categories of substances considered to be a TIER 1 HSSM.

Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM) - HSSM transported by motor vehicle whose potential consequences from an act of terrorism include moderately significant level of adverse effects on human life or health, environmental damage, transportation system disruption, or economic disruption. Attachment B contains a listing of categories of substances considered to be a TIER 2 HSSM.

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

The listing of Tier 1 and Tier 2 HSSM provided in Appendix B is not intended to meet the requirements to develop a list of security sensitive materials as defined in section 1501 of the Implementing Recommendations of the 9/11 Commission Act of 2007.

General Security:

- 1) **Security Assessment and Security Plan Requirements (TIER 1 HSSM, TIER 2 HSSM)** – Motor carriers are required by PHMSA regulations in 49 CFR Part 172, Subpart I to develop and implement security plans to address security risks related to the transportation of hazardous materials. TSA recommends that employers review their security assessment and determine the security action items which may be appropriate to address their assessed risks. To obtain further guidance on the security planning process, employers should review the Federal Motor Carrier Safety Administration (FMCSA) *Guide to Developing an Effective Security Plan* and the PHMSA document *Risk Management Self-Evaluation Framework (RMSEF)*. These guidance materials can be found on the FMCSA website at <http://www.fmcsa.dot.gov/> and the PHMSA website at <http://www.phmsa.dot.gov/>.
- 2) **Awareness of Industry Security Practices (TIER 1 HSSM, TIER 2 HSSM)** – Employers should become familiar with security practices recommended by industry groups and trade associations to further enhance transportation security. Examples include the American Chemistry Council's (ACC) Responsible Care Program, the Chlorine Institute's Security Management Plan, the International Cargo Security Council and other entities offering similar security guidance. Employers should review these security practices and consider their use in mitigating the assessed risks.
- 3) **Inventory Control Process (TIER 1 HSSM, TIER 2 HSSM)** – Employers should implement procedures to maintain accountability for their containers, cylinders, and vehicles at all times while in transport throughout the supply chain. Inventory control information should include: pertinent shipping information; material location; tracking processes; and verification procedures.
- 4) **Business and Security Critical Information (TIER 1 HSSM, TIER 2 HSSM)** – Employers should implement policies to protect security critical information. This policy should address current methods of communication between shippers, carriers, third-party logistic companies, and receivers. Information flow should be reduced to that which is essential to accomplish the task of transporting the hazardous material shipments. Communications and information systems should be protected from unauthorized access.

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

This includes telecommunications, computer systems, printed materials, verbal communications and all networks on which they operate.

Personnel Security:

- 5) **Possession of a Valid Commercial Drivers License-Hazardous Materials Endorsement (TIER 1 HSSM, TIER 2 HSSM)** – TSA is aware that motor carriers are required by Federal Motor Carrier Safety Administration (FMCSA) regulations in 49 CFR Part 383 to verify that a person employed to drive a vehicle containing hazardous materials (which includes TIER 1 HSSM and TIER 2 HSSM) has a valid commercial drivers license (CDL) with a hazardous materials endorsement (HME). A driver with a valid CDL with an HME will have undergone a Security Threat Assessment conducted by the Transportation Security Administration (TSA) under 49 CFR Part 1572. TSA is not recommending that drivers with HMEs undergo additional background checks under these voluntary action items.

- 6) **Background checks for highway transportation sector employees other than motor vehicle drivers with a valid CDL with hazardous materials endorsement (TIER 1 HSSM, TIER 2 HSSM)** – During the hiring process, an employer in the highway-related hazmat supply chain should conduct a background check for employees and contractors with unescorted access to motor vehicles (in transport), the motor carrier facility, or information critical to the hazmat transportation. Attachment A-1 provides guidance on the recommended scope and procedures for these voluntary background checks to include a criminal background check, verification of social security number, and verification of immigration status. An employer should also establish a method of redress as described in Attachment A-1. This SAI may also be satisfied by the CDL HME background check requirement or background checks mandated by other Government agencies, such as the ATF's Employee Possessor Questionnaire, provided that the background check meets or exceeds the guidance in Attachment A-1.

- 7) **Security Awareness Training for Employees (TIER 1 HSSM, TIER 2 HSSM)** – In support of the PHMSA security training requirements in 49 CFR 172.704, employers should have employees complete TSA-sponsored domain awareness training, the TSA Hazmat Motor Carrier Security Self-Assessment Training Program or other equivalent security training programs. For more information see www.tsa.gov/what_we_do/tsnm/highways.shtm Employers may wish to establish security awareness training programs that at a minimum address methods to: restrict access to sensitive information on HSSM such as shipping papers, dates of shipment and arrival, destination and routing information; recognize suspicious activities of potential terrorists; assess

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

vulnerabilities and apply security measures; and notify the appropriate authorities of unusual activities.

Unauthorized Access:

- 8) **Access Control System for Drivers (in addition to CDL) (TIER 1 HSSM, TIER 2 HSSM)** – Employers should implement an access control system that includes issuing company photo IDs or other visible forms of company identification to all drivers. These company IDs should be used by drivers to gain access to company designated restricted areas (such as vehicle key control room, loading or unloading processes) as appropriate, and also for shippers, consignees and others to verify the drivers' current employment status.

- 9) **Access Control System for Facilities Incidental to Transport (TIER 1 HSSM, TIER 2 HSSM)** – Employers should implement an access control system that includes issuing company photo IDs or other visible forms of employee identification to all employees, vendors, contractors, and visitors who require unescorted access to restricted areas on a permanent or temporary basis, as appropriate. This system should control access to restricted areas including plants, data centers and IT systems, loading and unloading facilities, storage facilities, and other critical areas as designated by company management. Company-issued ID cards and other forms of employee identification should be required to be displayed by the holder at all times while on company property. Employers should also establish a method of challenging individuals who do not display the appropriate identification. It is expected that such a system will be unnecessary at businesses with fewer than 10 employees.

En-route Security:

- 10) **Establish Communications Plan (TIER 1 HSSM, TIER 2 HSSM)** - A communication plan should be established to include standard operating procedures (SOP) for communications between drivers, appropriate company personnel, and emergency services agencies. This plan should include the appropriate two-way communication technologies required to implement the communication plan, such as terrestrial or satellite-based systems. This is not intended to preclude the use of personal cell phones. Employers should encourage and employees should follow the proper use of cell phones including observing state and local cell phone laws.

- 11) **Establish Appropriate Vehicle Security Program (TIER 1 HSSM, TIER 2 HSSM)** – Employers should ensure that all company vehicles (power units including but not limited to tractors, straight trucks, pickups, and

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

service units) are secured when unattended through use of a primary and secondary securement systems. Primary methods should include the following:

- a) Ensuring that all company vehicles have the capability to be locked.
- b) Adopt a written security policy that includes:
 - i) procedures such as a key control program when a vehicle is not in active use, and
 - ii) ensuring the vehicle engine is turned off, remove keys from vehicle, closing windows, and locking doors when the vehicle is in active use but unattended.

Secondary securement methods should include the following:

- a) Steering wheel locking system,
- b) Air brake locking system,
- c) Wheel locks, or
- d) Other appropriate lockout control process.

- 12) **Establish Appropriate Cargo Security Program to Prevent Theft or Sabotage of Cargo Containers (TIER 1 HSSM, TIER 2 HSSM) –** Employers should ensure that all cargo containers (including but not limited to trailers, tankers, straight trucks, security cages, and flatbeds) are secured when in use but unattended through use of a primary and secondary securement system. The primary methods should include the following:
- a) Ensuring that all cargo containers have the capability to be locked.
 - b) Adopt a written security policy that includes:
 - i) a key control program (if appropriate), and
 - ii) ensuring a container is provided with a mechanical or electrical method of locking.
- Secondary securement method should include the following:
- a) Glad hand locks,
 - b) King pin locks,
 - c) Wheel locks, or
 - d) Other appropriate lockout control process
- 13) **Implement a Seal/Lock Control Program to Prevent Theft or Sabotage of Cargo (TIER 1 HSSM, TIER 2 HSSM) –**Employers should implement a seal/lock program to prevent theft or sabotage of the contents of cargo containers and cylinders when in transport, when unattended by company personnel, or when at facilities incidental to transport. The following is recommended:
- Tier 1 HSSM – High security locks or electronic seals
 - Tier 2 HSSM – Tamper evident (indicative) seals.

When establishing a seal/lock control program employers should review the “User’s Guide on Security Seals for Domestic Cargo” (January 2007)

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

developed jointly by the Department of Homeland Security and Department of Defense. A copy of this document may be requested by sending electronic mail to highwaysecurity@dhs.gov.

- 14) **High Alert Level Protocols (TIER 1 HSSM, TIER 2 HSSM)** – Employers should establish policies governing operations during periods of increased threat conditions under the Homeland Security Advisory System (for example when the DHS Threat Condition is raised from Orange to Red). These protocols should be capable of being implemented when deemed appropriate by an employer or appropriate law enforcement or homeland security officials. Alternatives to continued routine operations include:
- a) Identifying secure locations to seek refuge,
 - b) For shipments exceeding 200 miles, identify private sector or law enforcement escorts to provide increased vehicle security, surveillance, and communications between local law enforcement officials and the motor vehicle while en route for shipments exceeding 200 miles or
 - c) Other appropriate security measures identified by the employer.

Examples of planning for secure locations include mutual agreements with industry partners and stakeholders or utilizing state weigh stations and inspection facilities that can provide law enforcement protection.

- 15) **Establish Security Inspection Policy and Procedures (TIER 1 HSSM, TIER 2 HSSM)** – Employers should establish a security inspection policy and procedures for drivers to conduct security inspections. Security inspections should be performed in conjunction with required safety inspections conducted under 49 CFR Part 392 before operation of the vehicle. These security inspections should occur initially at the beginning of the driver's shift or trip (pre-departure) and after any stop en-route in which the vehicle is left unattended. The security inspection should consist of all areas where a suspicious item could be placed, training to recognize suspicious items, and reporting and response procedures to follow if a suspicious item or package is found.
- 16) **Establish Reporting Policy and Procedures (TIER 1 HSSM, TIER 2 HSSM)** – Employers should implement reporting procedures for drivers and non-driver employees to follow when reporting suspicious incidents, threats, or concerns regarding transportation facilities (terminal, distribution center, etc.) or company vehicles. These procedures should include at a minimum; appropriate company points of contact, appropriate law enforcement agencies, and the appropriate emergency response telephone number required in 49 CFR 172.604 and 172.606.

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

- 17) **Shipment Pre-Planning, Advance Notice of Arrival and Receipt Confirmation Procedures with Receiving Facility (TIER 1 HSSM only)**
– The shipper (consignor), motor carrier and receiver (consignee) should conduct shipment pre-planning to ensure shipments are not released to the motor carrier until they can be transported to destination with the least public exposure and minimal delay in transit. Shipment pre-planning should include establishing the estimated time of arrival (ETA) agreeable to consignor, motor carrier, and consignee; load specifics (shipping paper information), and driver identification. When shipments are in transit, the motor carrier should coordinate with consignee to confirm the pre-established ETA will be met, or agree on a new ETA. Upon receipt of the shipment consignees should notify the shipper that the shipment has arrived on schedule and materials are accounted for. Methods for advance notice and confirmation of receipt of shipments include electronic mail and voice communications. When practical, consignees should immediately alert the appropriate shipper or motor carrier if the shipment fails to arrive on schedule or if a material shortage is discovered. Methods for immediate alert notifications should be made by voice communications only. Where immediate notification is not practical (for example at unmanned facilities), the consignor, the motor carrier, and consignee should agree on alternate confirmation (method and time) of delivery and receipt. Consignees should make every effort possible to accept a shipment that arrives during non-business hours due to unforeseen circumstances.
- 18) **Preplanning Routes (TIER 1 HSSM only)** – Employers should ensure preplanning of primary and alternate routes. This preplanning should seek to avoid or minimize proximity to highly populated urban areas or critical infrastructure such as bridges, dams, and tunnels. Policies governing operations during periods of Orange or Red alert levels under the Homeland Security Advisory System should plan for alternate routing for TIER 1 HSSM shipments away from highly populated urban areas and critical infrastructure. The motor carrier or law enforcement officials may determine when to implement alternate routing. Drivers should be encouraged to notify the company’s dispatch center when substantial or non-routine deviation from the route is necessary.
- 19) **Security for Trips Exceeding Driving Time under the Hours of Service of Drivers Regulation (49 CFR Part 395) - (TIER 1 HSSM only)** – Employers should examine security in light of hours of service available and take steps to mitigate the vulnerabilities associated with extended rest stops for driver relief. Examples include methods such as constant vehicle attendance or visual observation with the vehicle, driver teams, or vetted companions. Other examples include arranging secure locations along the route through mutual agreement with industry partners and stakeholders, or

Appendix A
Description of Voluntary Security Action Items for
Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)

State weigh stations and inspection facilities that provide law enforcement protection.

- 20) **Dedicated Truck (TIER 1 HSSM only)** –Employers should implement policies to ensure that, except under emergency circumstances, contracted shipments remain with the primary carrier and are not subcontracted, driver/team substitutions are not made, and transloading does not occur unless the subcontractor has been confirmed to comply with applicable Federal safety and security guidance and regulations and company security policies.
- 21) **Tractor Activation Capability (TIER 1 HSSM only)** –Employers should implement security measures that require driver identification by login and password or biometric data to drive the tractor. Companies should provide written policies and instructions to drivers explaining the activation process.
- 22) **Panic Button Capability (TIER 1 HSSM only)** –Employers should implement means for a driver to transmit an emergency alert notification to dispatch. “Panic Button” technology enables a driver to remotely send an emergency alert notification message either via Satellite or Terrestrial Communications, and/or utilize the remote Panic Button to disable the vehicle.
- 23) **Tractor and Trailer Tracking Systems (TIER 1 HSSM only)** – Employers should have the ability of implementing methods of tracking the tractor and trailer throughout the intended route with satellite and/or land-based wireless GPS communications systems. Tracking methods for the tractor and trailer should provide current position by latitude and longitude. Geofencing and route monitoring capabilities allow authorized users to define and monitor routes and risk areas. If the tractor and/or trailer deviates from a specified route or enters a risk area, an alert notification should be sent to the dispatch center. An employer or an authorized representative should have the ability to remotely monitor trailer “connect” and “disconnect” events. Employers or an authorized representative should have the ability to poll the tractor and trailer tracking units to request a current location and status report. Tractor position reporting frequency should be configured at not more than 15-minute intervals.

Trailer position reporting frequency should be configured to provide a position report periodically when the trailer has been subject to an unauthorized disconnect from the tractor. The reporting frequency should be at an interval that assists the employer in locating and recovering the trailer in a timely manner. The tractor and trailer tracking system should be tested periodically and the results of the test should be recorded.