



The North American Transportation Security Center

Report Number: KTC-19-24/FD01-1F

DOI: <https://doi.org/10.13023/ktc.rr.2019.24>



Kentucky Transportation Center
College of Engineering, University of Kentucky, Lexington, Kentucky

in cooperation with
Kentucky Transportation Cabinet
Commonwealth of Kentucky

The Kentucky Transportation Center is committed to a policy of providing equal opportunities for all persons in recruitment, appointment, promotion, payment, training, and other employment and education practices without regard for economic, or social status and will not discriminate on the basis of race, color, ethnic origin, national origin, creed, religion, political belief, sex, sexual orientation, marital status or age.

Kentucky Transportation Center
College of Engineering, University of Kentucky, Lexington, Kentucky

in cooperation with
Kentucky Transportation Cabinet
Commonwealth of Kentucky

© 2018 University of Kentucky, Kentucky Transportation Center
Information may not be used, reproduced, or republished without KTC's written consent.

Research Report
KTC-19-24/FD01-1F

The North American Transportation Security Center

Doug Kreis, Ph.D.
Associate Director

and

Michael Barclay
Coldstream Digital

Kentucky Transportation Center
College of Engineering
University of Kentucky
Lexington, Kentucky

In Cooperation With
Kentucky Transportation Cabinet
Commonwealth of Kentucky

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the University of Kentucky, the Kentucky Transportation Center, the Kentucky Transportation Cabinet, the United States Department of Transportation, or the Federal Highway Administration. This report does not constitute a standard, specification, or regulation. The inclusion of manufacturer names or trade names is for identification purposes and should not be considered an endorsement.

December 2008

Table of Contents

1.0 Project Overview	1
2.0 Regulatory & Legislative Drivers	5
2.1 How does the Federal government regulate the transportation of hazardous waste and hazardous materials?	
2.2 Hazmat security is driving the development of new regulations.	
2.2.1 Shippers and carriers of certain hazardous materials must prepare security plans and conduct security training (RSPA).	
2.2.2 States must perform security checks before licensing hazmat drivers (DHS).	
2.2.3 Carriers of security-sensitive hazardous materials must obtain a hazmat safety permit (FMCSA).	
2.2.4 Chemical facility anti-terrorism standards focus on hazmat security (DHS).	
2.3 In 2007, TSA assumed the lead federal responsibility for hazmat transportation security rulemaking.	
2.4 TSA issued guidance for shippers and carriers of highway security-sensitive materials on June 26, 2008.	
2.4.1 TSA's security recommendations incorporate/enhance earlier DOT guidance.	
2.4.2 TSA recommends more stringent security measures for Tier 1 highway security-sensitive shipments.	
2.5 The 9/11 Commission Act of 2007 (PL 110-53/H.R. 1) requires TSA to take action on hazmat truck tracking.	
2.5.1 Earlier legislative initiatives paved the way for PL 110-53.	
2.5.2 PL 110-53 requires TSA to develop a hazmat truck tracking program.	
2.5.3 PL 110-53 requires DHS to evaluate hazmat truck routes.	
2.5.4 TSA plans to expand on the recently completed Hazmat Truck Security Pilot program.	
2.6 EPA wants to implement a hazardous waste electronic manifest program.	
2.6.1 EPA's hazardous waste manifest requirements are burdensome and expensive.	
2.6.2 Electronic manifests have the potential of generating savings of more than \$300 million/year.	
2.6.3 EPA wants to build a national hazardous waste e-manifest processing center using a public/private partnership.	
2.6.3.1 EPA's original electronic manifest NPRM in 2001 established basic e-manifest requirements.	
2.6.3.2 EPA held a public meeting in May 2004 to discuss the future of its e-manifest program.	
2.6.3.3 EPA's uniform manifest rule and its Cross Media Environmental Reporting Rule (CROMERR) laid the foundation for an e-manifest rule.	
2.6.3.4 EPA's attempt to use GSA's Share-In-Savings contract program in 2005 was unsuccessful.	
2.6.3.5 EPA's Public Notice (<i>Federal Register</i> April 18, 2006) reaffirmed EPA's intent to use a public/private partnership.	
2.6.3.6 EPA supported an unsuccessful legislative attempt to gain "share-in-savings" type authority (Senate Bill 3871 – 109 th Congress September 2006).	
2.6.3.7 EPA's Notice of Data Availability (<i>Federal Register</i> February 26, 2008) reaffirmed EPA's intent to seek a public/private partnership via e-manifest legislation.	
2.6.3.8 Senate Bill 3109, Hazardous Waste Manifest Establishment Act, was introduced by Senator John Thune (R-SD) on June 10, 2008	
2.7 The Alliance for Uniform Hazmat Transportation Procedures was established by state agencies to preserve state prerogatives in hazmat registration and permitting.	

- 2.7.1 Why was the Alliance established?
 - 2.7.2 What is the Uniform Program?
 - 2.7.2.1 The Uniform Program revolves around the “base state” concept.
 - 2.7.2.2 Under the Uniform Program, hazmat carriers must have acceptable safety and operating records.
 - 2.7.2.3 Hazmat fees are allocated using the double apportionment method.
 - 2.7.2.4 What data do Alliance states collect from carriers during registration and permitting?
 - 2.7.3 What requirements does a state have to meet to join the Alliance?
 - 2.7.4 What oversight does the Alliance exercise over member programs?
 - 2.7.5 What are the benefits of state membership in the Alliance? Why is membership lagging?
- 2.8 How will these regulatory/legislative drivers influence the design and operation of the Transportation Security Center?

3.0 Technology Drivers 47

- 3.1 “Smart Truck” technology, a core component of a hazmat tracking system, is inexpensive and available from numerous vendors.
 - 3.1.1 A GPS receiver and a wireless modem are core building blocks of a “smart truck” system.
 - 3.1.2 The smart truck market is well developed and well served.
- 3.2 Truck-based asset tracking systems are key components of corporate RFID/supply chain systems.
- 3.3 IEEE’s 1512 family of XML messaging standards supports intelligent transportation systems.
- 3.4 Service-oriented architectures integrate business processes.
- 3.5 The E-Sign law of 2000 gave electronic transactions the same legal weight as paper-based transactions.
 - 3.5.1 Electronic (XFML) forms satisfy public and private digital business needs.
 - 3.5.2 Digital signatures ensure document integrity and prevent signature repudiation by system users.
- 3.6 Internet-based businesses can be located almost anywhere.
- 3.7 Business rules engines provide sophisticated analyses of market conditions on a dynamic basis.
- 3.8 Web-based crisis information management software supports “virtual” operations centers; enhances communication during an incident.
- 3.9 Agile software development allows project teams to “develop quickly and deliver often”.
- 3.10 How will these technology drivers influence the design and operation of the Transportation Security Center?

4.0 Lessons Learned (Experience Drivers)..... 67

- 4.1 U.S. Federal Motor Carrier Safety Administration - Hazardous Materials Safety and Security Technology Field Operational Test
 - 4.1.1 How was “smart truck” technology deployed in the FOT?
 - 4.1.2 How does “smart truck” technology deployment affect carrier costs?
 - 4.1.3 What is the ROI for “smart truck” technology deployment?
 - 4.1.4 How big is the market for “smart truck” technology deployment?
 - 4.1.5 How will “smart truck” technology deployment affect carrier profits?
 - 4.1.6 What methodology did the FOT project team use to calculate security benefits?

- 4.1.7 What is the Public Sector Reporting Center (PSRC)? What implementation issues are associated with the PSRC?
- 4.1.8 What observations did FOT study participants take out of the field experience?
- 4.2 The U.S. Federal Motor Carrier Safety Administration - Untethered Trailer Tracking Systems
 - 4.2.1 How do UTT systems work?
 - 4.2.2 The FMCSA developed functional specifications for UTT systems and conducted a field test of commercial trailer tracking systems.
 - 4.2.3 What are the benefits/costs of UTT?
 - 4.2.4 Who offers UTT products and services?
- 4.3 U.S. Federal Motor Carrier Safety Administration – Vehicle Immobilization Systems
 - 4.3.1 What is a vehicle immobilization system?
 - 4.3.1.1 Remote disabling systems enable a control center to prevent a truck from being used by an unauthorized driver or to stop a moving truck.
 - 4.3.1.2 Non-remote disabling systems enable authorized drivers to stop a moving truck; prevents unauthorized drivers from driving the truck.
 - 4.3.2 The FMCSA evaluated vehicle immobilization systems and developed functional requirements.
 - 4.3.3 What are the benefits/costs of vehicle immobilization?
 - 4.3.4 Who offers vehicle immobilization systems?
- 4.4 Singapore Civil Defence Force - Hazmat Transport Vehicle Tracking System
 - 4.4.1 Why did Singapore build the HTVTS?
 - 4.4.2 Singapore’s regulations drive technology deployment.
 - 4.4.3 What is the technology behind the HTVTS?
 - 4.4.4 How does the SCDF factor risk assessment into its hazmat tracking program?
 - 4.4.5 How does the HTVTS fit into Singapore’s overall hazmat management program?
- 4.5 U.S. Transportation Security Administration - Hazmat Truck Security Pilot
 - 4.5.1 What are the building blocks of a hazmat truck tracking center?
 - 4.5.2 Shippers, carriers, and truck tracking vendors have to deploy “smart truck” technology and submit data to enable a truck tracking center.
 - 4.5.3 The HTSP prototype design reflected assumptions about technology deployment and data reporting.
- 4.6 U.S. Customs & Border Protection – ACE Truck E-Manifest
 - 4.6.1 E-manifests and RFID systems speed trucks past CBP inspection stations.
 - 4.6.2 Carriers can use CBP’s portal to submit a truck e-manifest; CBP’s e-manifest has 70 data elements.
- 4.7 Ontario Ministry of the Environment - Hazardous Waste Information Network
 - 4.7.1 What is Ontario’s Regulation 347? Why was it enacted?
 - 4.7.2 What is the Hazardous Waste Information Network? How does it support Regulation 347?
 - 4.7.3 Who are the system users? How do they use HWIN?
 - 4.7.3.1 HWIN was built around the regulatory needs of waste generators.
 - 4.7.3.2 Waste transporters and waste management firms also use HWIN.
 - 4.7.3.3 MOE uses HWIN to support a variety of administrative and operational functions.
 - 4.7.4 What service/operational problems did MOE experience during HWIN implementation?
 - 4.7.5 Waste generators and waste firms did not make a move to e-manifests.

- 4.8 The Commission for Environmental Cooperation (NAFTA Environmental Commission) envisions a North American waste tracking system.
- 4.9 Taiwan Environmental Protection Administration - Hazardous Waste and Hazmat Shipment Tracking
- 4.10 How will these experience drivers influence the design and operation of the Transportation Security Center?

5.0 Business Drivers..... 119

- 5.1 Hazmat shipment tracking – the top five business drivers
 - 5.1.1 The 9/11 Commission Act of 2007 (PL 110-53/H.R. 1) requires TSA to take action on hazmat truck tracking.
 - 5.1.2 There is public demand for a secure hazmat supply chain.
 - 5.1.3 Security is driving technology innovation in the hazmat truck security market; the market anticipates a government regulatory program.
 - 5.1.4 “Smart truck” technology deployment saves hazmat carriers money; generates huge benefits for the public.
 - 5.1.5 Technology is not an inhibiting factor for a truck tracking center; developing an effective regulatory/implementation framework is the challenge.
- 5.2 Hazardous waste e-manifests – the top five business drivers
 - 5.2.1 EPA wants hazardous waste trading partners to use e-manifests.
 - 5.2.2 E-manifests will unlock cost savings for government and industry.
 - 5.2.3 E-manifest cost savings provide revenue opportunity for state agencies.
 - 5.2.4 Hazardous waste management is a state-delegated program.
 - 5.2.5 Technology is not an inhibiting factor for a hazardous waste e-manifest processing center; developing an effective business, regulatory, and implementation framework is the challenge.
- 5.3 Business drivers common to both hazmat and hazardous waste
 - 5.3.1 The transportation of hazardous materials and hazardous waste is a highly regulated business.
 - 5.3.2 EPA’s proposed transaction revenue model supports establishment of a for-profit business for hazmat shipment tracking and hazardous waste e-manifest processing.
 - 5.3.3 Government agencies are increasingly interested in privatization.
 - 5.3.4 Financial considerations and programmatic/technology overlaps argue for co-location of TSA’s hazmat truck tracking center and EPA’s hazardous waste e-manifest processing center.

6.0 Regulatory Program Plan..... 125

- 6.1 Kentucky’s hazmat supply chain is an attractive target for terrorists.
- 6.2 Kentucky should seek membership in the Alliance for Uniform Hazmat Transportation Procedures.
- 6.3 Recommended regulatory strategy
 - 6.3.1 Kentucky’s model program will support implementation of PL 110-53 (Tier 1 HSSM tracking).
 - 6.3.2 Kentucky’s model program will support implementation of EPA’s hazardous waste e-manifest program.
 - 6.3.3 Kentucky’s model program will position Kentucky to host the Transportation Security Center and establish the Transportation Security Center as a for-profit business.
 - 6.3.4 Kentucky’s model program will support Kentucky’s entry into the Alliance for Uniform Hazmat Transportation Procedures.
- 6.4 Critical elements of the model regulatory programs
 - 6.4.1 Tier 1 HSSM shipment tracking

- 6.4.1.1 Shipments of TSA-designated Tier 1 highway security-sensitive shipments (HSSMs) are "regulated shipments".
 - 6.4.1.2 Tier 1 HSSM shipments traveling over Kentucky's roads must meet Kentucky's hazmat shipment security requirements.
 - 6.4.1.3 Carriers of Tier 1 HSSM shipments must install smart truck devices that are Transportation Security Center compliant.
 - 6.4.1.4 Shippers and carriers of Tier 1 HSSM must register with the Transportation Security Center.
 - 6.4.1.5 The shipper or carrier of a Tier 1 HSSM shipment must file an electronic manifest with the Transportation Security Center before the regulated shipment may leave a shipper's facility.
 - 6.4.1.6 The shipper or carrier of a Tier 1 HSSM shipment must file an electronic route plan with the Transportation Security Center before a regulated shipment may leave a shipper's facility.
 - 6.4.1.7 Carriers of Tier 1 HSSM shipments must use the services of a fleet tracking vendor that has Transportation Security Center compliant systems and service offerings.
 - 6.4.1.8 A carrier's fleet tracking vendor must report the location of a carrier's vehicle hauling a regulated shipment to the Transportation Security Center in a manner and at a polling frequency specified by the Transportation Security Center.
 - 6.4.1.9 The truck tracking vendor must report certain alerts and messages from installed smart truck devices on the carrier's vehicle to the Transportation Security Center in a manner specified by the Transportation Security Center.
 - 6.4.1.10 Shippers and carriers of Tier 1 HSSM shipments must respond to inquiries and alerts issued by the Transportation Security Center.
 - 6.4.1.11 A carrier and the Transportation Security Center must have the ability to verbally communicate with a driver hauling a regulated shipment.
 - 6.4.1.12 A carrier must provide drivers of Tier 1 HSSM shipments the ability to send a panic alert both in and out of the cab.
 - 6.4.1.13 A Tier 1 HSSM shipper may not release a regulated shipment to a driver that does not have a CDL with a hazmat extension or a FMCSA or state-issued hazmat safety permit.
 - 6.4.1.14 Shippers must pay a homeland security fee for each Tier 1 HSSM shipment as well as other regulatory fees established by the state.
- 6.4.2 Hazardous waste electronic manifest
- 6.4.2.1 Waste generators, transporters, and TSDFs may use electronic manifests instead of paper manifests.
 - 6.4.2.2 Hazardous waste shipments originating or ending in Kentucky are subject to Kentucky's hazardous waste electronic manifest regulations.
 - 6.4.2.3 Waste generators, transporters, and TSDFs must register with the Transportation Security Center.
 - 6.4.2.4 A waste generator may not release a hazardous waste shipment to a driver that does not have a CDL with a hazmat extension.
 - 6.4.2.5 Hazardous waste electronic manifest transactions must be processed through the Transportation Security Center.
 - 6.4.2.6 Waste generators and TSDFs must pay regulatory fees established by EPA or the state.
 - 6.4.2.7 Use of electronic manifests is voluntary however parties to the manifest transaction will pay higher regulatory fees for paper manifest processing.
 - 6.4.2.8 A waste transporter may serve as an "offeror" and sign a manifest on behalf of the waste generator.
 - 6.4.2.9 A waste transporter is not required to install smart truck devices or use a fleet tracking vendor but it is strongly encouraged (optional regulatory element).

- 6.5 Kentucky Statutes and Regulations
 - 6.5.1 Current statutes and regulations
 - 6.5.1.1 Kentucky’s hazardous materials program
 - 6.5.1.2 Kentucky’s hazardous waste program
 - 6.5.2 Recommended statutory refinements – Tier 1 HSSM tracking
 - 6.5.3 Recommended statutory refinements - hazardous waste electronic manifest

7.0 The North American Transportation Security Center..... 145

- 7.1 The North American Transportation Security Center will operate as a for-profit business; will use the EPA-inspired transaction fee revenue model.
- 7.2 The North American Transportation Security Center will serve as TSA’s hazmat truck tracking center.
- 7.3 The North American Transportation Security Center will serve as EPA’s hazardous waste electronic manifest processing center.
- 7.4 The hazmat truck tracking services offered by the North American Transportation Security Center will operate under the FedTrak.com™ brand name.
- 7.5 FedTrak.com™ will provide truck tracking services for shipments of TSA-designated Tier 1 Highway Security-Sensitive Materials.
- 7.6 Tier 1 HSSM carriers must use the services of a FedTrak.com™ certified hazmat truck tracking vendor.
- 7.7 Tier 1 HSSM carriers must install FedTrak.com™ compliant “smart truck” technology devices on their vehicles.
- 7.8 Incident management will follow a defined workflow.
- 7.9 Shippers of Tier 1 HSSMs will pay a homeland security fee for each “gate out” to “gate-in” transaction.
- 7.10 The hazardous waste electronic manifest services offered by the North American Transportation Security Center will operate under the FedWaste.com™ brand name.
- 7.11 FedWaste.com™ will be EPA CROMERR-compliant and will serve as a node on EPA’s Central Data Exchange (CDX) system.
- 7.12 FedWaste.com™ will integrate the business processes of waste generators, transporters, and waste firms.
- 7.13 FedWaste.com™ will collect a transaction fee for processing an e-manifest on behalf of EPA or a state agency.
- 7.14 FedWaste.com™ will provide the states a mechanism to implement regulatory fee programs and to efficiently collect payments.
- 7.15 E-manifest regulatory fees will be paid by waste generators and waste firms; can be a significant revenue source for states.
- 7.16 FedWaste.com™ will operate a paper manifest processing center in conjunction with FedWaste.com™ to support EPA’s new “offeror” regulatory provision.
- 7.17 Higher transaction fees for paper manifests will promote e-manifest use.

Appendices

Appendix A	U.S. EPA Hazardous Waste Manifest Regulations and Business Processes
Appendix B	TSA List of Highway Security-Sensitive Materials (June 26, 2008)
Appendix C	High Level Plan for Implementing H.R. 1 (Transportation Sector Network Management; Highway Motor Carrier Programs Office; U.S. Transportation Security Administration); March 2008
Appendix D	FMCSA Functional Specifications for Untethered Trailer Tracking Systems
Appendix E	Singapore HazMat Transport Vehicle Tracking System (Case Study)
Appendix F	Kentucky Hazmat Supply Chain Threat Analysis
Appendix G	Kentucky Statutes and Regulations

List of Figures

Figure 2.2.a	Timeline – Hazmat Security Regulations and Legislation
Figure 2.2.b	DOT's En-Route Security Guidance for Hazmat Shippers
Figure 2.2.b	Relationship between HM-232 and the chemical industry's Responsible Care® program
Figure 2.2.d	Number of carriers requiring FMCSA hazmat safety permits.
Figure 2.4.a	Implications of EPA's Hazardous Waste E-Manifest Program for the Transportation Security Center.
Figure 2.6.a	Timeline for EPA's electronic manifest initiative
Figure 2.7a	The Alliance for Uniform Hazmat Transportation Procedures
Figure 2.7.b	Data Collected from Carriers by Alliance States
Figure 2.8.a	Implications of regulatory/legislative drivers on the design and operation of the Transportation Security Center
Figure 3.1.a	Truck-mounted "smart truck" devices are connected to a commercial fleet tracking center by a wireless modem on the truck making the truck a "rolling office".
Figure 3.11.a	Implications of technology drivers on the Transportation Security Center
Figure 3.1.b	Truck tracking vendors offer an impressive list of smart truck products and services.
Figure 4.1.a	FOT "Smart Truck" Technology Deployment
Figure 4.1.b	Estimated Monthly Per Truck Operational Benefits by Using Wireless Communications With GPS Vehicle Positioning System
Figure 4.1.c	Per Truck-Specific Technology Costs (Wireless Communications with GPS Tracking Capabilities)
Figure 4.1.d.	Costs, Benefits, Benefit-Cost Ratios, and Payback Periods by Industry Segment (Wireless Communications with GPS Tracking Capabilities)
Figure4.1.e	"Smart Truck" Technology Deployment Levels
Figure 4.1.f.	Full Deployment Investment - Industry Efficiency Benefit and Cost Estimates/Investments Over 3 Years - Wireless with GPS (In Millions of Dollars)
Figure 4.1.g.	Percent reduction in overall vulnerability by load type and technology.
Figure 4.1.h.	Reasonable Worst-Case Per Attack Consequences

- Figure 4.1.i. Estimated Security Benefits (In Millions of Dollars)
- Figure 4.1.j. Implementation issues with the Hazmat PSRC
- Figure 4.2.a The market for UTT products is served by a number truck tracking vendors.
- Figure 4.3.a Technology components of a vehicle immobilization system.
- Figure 4.3.b Vehicle immobilization system vendors
- Figure 4.4.a Hazmat Transport Vehicles Truck Security Immobilization System
- Figure 4.4.b Approved Hazmat Transportation Routes in Singapore
- Figure 4.5.a Building blocks of a hazmat truck tracking center.
- Figure 4.5.b The HTSP project began October 2005 and ended April 2008.
- Figure 4.6.a. ACE Truck E-Manifest.
- Figure 4.6.b. ACE Truck E-Manifest Benefits
- Figure 4.7.a. My HWIN Page
- Figure 4.7.b MOE's paper manifest processing business process.
- Figure 4.4.7.c Reasons for Low E-Manifest Use in Ontario
- Figure 4.9.a Taiwan's Industrial Waste Control Center
- Figure 6.4.a TSA Tier 1 Highway Security Sensitive Materials
- Figure 7.a Hazmat tracking at the North American Transportation Security Center
- Figure 7.8 FedTrak.com™ incident management workflow

1.0 Project Overview

There are over 800,000 hazardous materials (hazmat) shipments over the nation's roads each day. According to the **U.S. Department of Homeland Security (DHS)**, terrorist activity related to the transportation of hazardous materials represents a significant threat to public safety and the nation's critical infrastructure. Specifically, the federal government has pointed to the government's inability to track hazmat shipments on a real-time basis as a significant security vulnerability.

In 2004, the **U.S. Federal Motor Carrier Safety Administration (FMCSA)** completed a study to determine if "smart truck" technology such as GPS tracking, wireless modems, panic buttons, and on-board computers could be used to enhance hazmat shipment security. The FMCSA study concluded that smart truck technology will be highly effective in protecting hazmat shipments from terrorists. The FMCSA study also concluded that smart truck technology deployment will produce a huge security benefit and an overwhelmingly positive return on investment for hazmat carriers.

The FMCSA study led to the **U.S. Transportation Security Administration's (TSA) Hazmat Truck Security Pilot**. This congressionally mandated pilot program was undertaken to demonstrate if a hazmat truck tracking center was feasible from a technology and systems perspective and to determine if existing truck tracking systems can interface with government intelligence centers and first responders. The Hazmat Truck Security Pilot demonstrated that a hazmat truck tracking center is feasible and in August 2007, Congress enacted legislation that directs TSA to develop a program - consistent with the Hazmat Truck Security Pilot - to facilitate the tracking of motor carrier shipments of security-sensitive materials.

In a different initiative, the **U.S. Environmental Protection Agency** is interested in implementing an electronic manifest rule that would allow companies to use electronic manifests instead of paper manifests for their hazardous waste shipments. Hazardous waste is a small subset of the much larger hazmat universe and the transportation of hazardous waste is co-regulated by EPA and the **U.S. Department of Transportation**. EPA and DOT regulations recognize EPA's hazardous waste manifest as satisfying DOT's hazmat shipping paper requirement. EPA estimates that the use of electronic manifests instead of paper manifests has the potential to generate over \$300 million/year in cost savings. EPA has expressed strong interest in using a public/private partnership to build a national hazardous waste electronic manifest processing center. Under this approach, a private party would build and operate the processing center at its own expense and collect a transaction fee for processing electronic manifests.

The **Kentucky Transportation Center (KTC)** of the University of Kentucky led a project funded by DHS via the Southeast Region Research Initiative (SERRI) to evaluate TSA and EPA needs. SERRI is managed by **BWXT Y-12** of Oak Ridge, TN. KTC project partners for the SERRI project were: **Morehead State University** (Morehead, KY); **Coldstream Digital LLC** (Lexington, KY; Great Falls, VA); **General Dynamics Advanced Information Systems** (Buffalo, NY), and **ThoughtWorks Inc.** (Chicago, IL).

KTC's SERRI project began August, 2007 and was completed October 2008. The project was designed to assess the feasibility of establishing the **North American Transportation Security Center** in Kentucky. The Transportation Security Center, as envisioned by the KTC project team, will serve as the implementing tool for a model hazmat regulatory program in Kentucky that will require:

- high-risk hazmat transporters to install "smart truck" technology on their vehicles;
- shippers and carriers to send electronic manifests and electronic route plans to the Transportation Security Center;
- carriers to report vehicle location and alerts to the Transportation Security Center (real-time XML data feed); and
- companies to pay hazmat regulatory fees.

The Transportation Security Center will also serve as the implementing tool for a model hazardous waste electronic manifest regulatory program.



Federal Motor Carrier Safety Administration seminal study – "smart truck" technology and hazmat shipment security.



TSA demonstrated that a truck tracking system is feasible. PL 110-53 directs TSA to develop a truck tracking program.



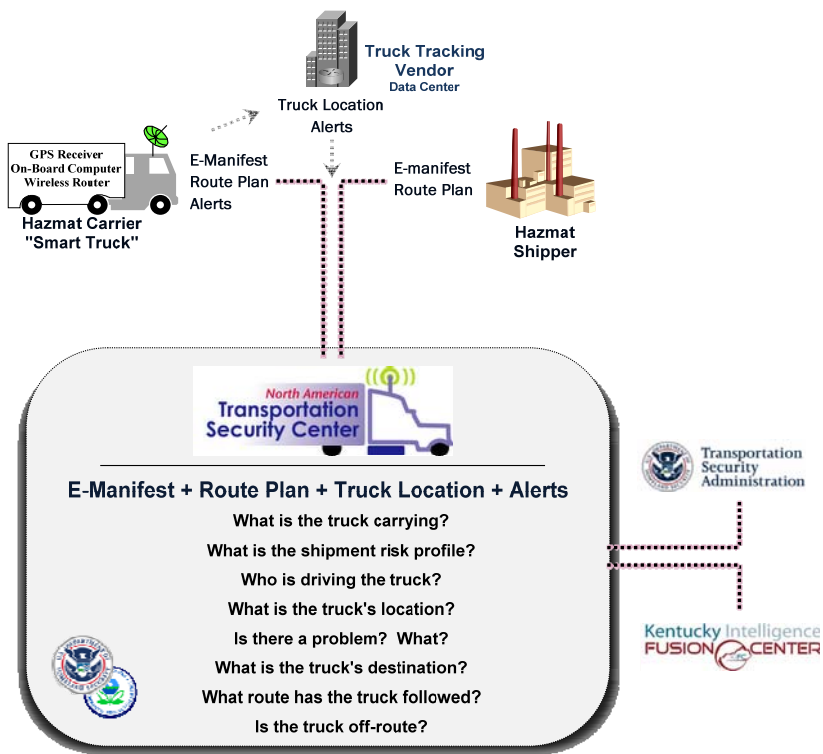
Hazardous waste is a subset of the much larger hazardous materials universe. Waste shipments are co-regulated by DOT and EPA.



DHS's Southeast Region Research Initiative funded the North American Transportation Security Center project.

Figure 1.a illustrates the hazmat tracking features of the Transportation Security Center. A “smart truck” equipped with an on-board computer, GPS receiver, and a wireless modem will use an internet connection (satellite or cellular) to interact with the Transportation Security Center and a commercial fleet tracking data center. E-manifest transactions between the carrier and the Transportation Security Center will provide the Transportation Security Center with information on the types and quantities of materials the transporter is hauling as well as shipment status (i.e. awaiting pickup, in transit, etc.). Data from the carrier’s fleet tracking data center will provide the Transportation Security Center the carrier’s exact location at all times. The shipper and/or carrier will also submit route plans. Alerts from the shipper or carrier will be generated when different events occur. The Transportation Security Center will merge e-manifest, vehicle location, route and alert data to provide government officials real-time visibility into the security status of hazmat shipments. In the event of a security incident, the Transportation Security Center will interact with State and Federal operations centers Kentucky’s Intelligence Fusion Center is the state action agency in the Commonwealth.

Figure 1.a Hazmat tracking at the North American Transportation Security Center.



The North American Transportation Security Center will merge information on shipment and vehicle location to enable real-time shipment tracking.

The project team examined four types of market “drivers” that influence the design and operation of the North American Transportation Security Center. They are:

- regulatory and legislative drivers;
- technology drivers;
- lessons learned (experience drivers); and
- business drivers.

Market driver analyses supported development of plans for the design and operation of the Transportation Security Center as well as plans for a model regulatory program. The project team prepared four deliverables.

1. A **high-level systems plan** for the North American Transportation Security Center describes how Transportation Security Center systems will be structured and how they will function.

2. A **concept of operations plan** for the North American Transportation Security Center describes the needs the Transportation Security Center will satisfy and how it will be structured to meet those needs.

3. A **regulatory program plan** presents model statutes/regulations that would be implemented in conjunction with hazmat tracking and hazardous waste electronic manifest programs by Kentucky's Cabinet agencies.

4. Recommendations regarding Kentucky's **membership in the Alliance for Uniform Hazmat Transportation Procedures** (the Alliance) are presented. The Alliance is a state-based organization sponsored by the National Conference of State Legislatures (NCSL) and established in conjunction with the FMCSA. The Alliance has established uniform procedures for state hazmat registration and permitting programs. Three states bordering Kentucky – Ohio, West Virginia, and Illinois – are Alliance members.



2.0 Regulatory & Legislative Drivers

This section examines regulations and legislation that will drive the design and operation of the North American Transportation Security Center.

Section 2.1 examines how the Federal government regulates the transportation of hazardous waste and hazardous materials. Sections 2.2 – 2.6 describe how hazmat truck security concerns are influencing recent federal hazmat transportation regulations and legislation. Included in this examination is an analysis of PL 110-53, the 9/11 Commission Act of 2007, that requires TSA to implement a hazmat truck security program.

Section 2.6 describes EPA's efforts to improve the current hazardous waste manifest process by introducing electronic manifests to the manifest business process.

Section 2.7 examines how states are managing their hazmat permitting and licensing programs through membership in the Alliance for Uniform Hazmat Transportation Procedures, an organization affiliated with the National Conference for State Legislatures.

2.1 How does the Federal government regulate the transportation of hazardous waste and hazardous materials?

Hazardous materials include many products in commerce such as chemicals, bulk fuels, and other materials requiring special care during transport. There are over *800,000 hazardous material shipments per day* over the U.S. road system including 75,000 shipments by tanker trucks.

The United States **Department of Transportation** (DOT) is responsible for regulating the transportation of all hazardous materials including hazardous waste. DOT's hazmat regulations cover: ¹

- preparation of a package for transportation (e.g., packaging, marking, labeling);
- preparation of shipping papers (e.g. to accompany hazmat shipment);
- hazmat storage incidental to transportation;
- hazmat vehicle loading and preparation (e.g. placarding);
- movement of the hazmat vehicle over the road system; and
- hazmat vehicle unloading at the ultimate consignee.

According to the U.S. **Department of Homeland Security** (DHS), terrorist activity related to the transportation of hazardous materials represents a significant threat to public safety and the nation's critical infrastructure. A typical gasoline tanker truck, for example, carries as much fuel as the jets that hit the World Trade Center and could be used by terrorists as a weapon of mass destruction. DHS and other federal agencies have initiated a number of efforts to secure the nation's hazardous materials supply chain against terrorist threats. Under the Patriot Act, DHS requires background checks and special state licensing for hazmat drivers. In 2003, DOT issued regulations for hazmat *shippers and carriers that require implementation of security plans, including training for employees.* In late 2004, DOT/FMCSA completed a study to determine how "smart truck" technology such as GPS tracking, panic buttons, and on-board computers could be used to enhance hazmat shipment security.

Despite the efforts made to date in securing hazmat shipments, it is notable that neither federal nor state governmental officials can track the location or movement of hazardous materials over the nation's highway system on a real-time basis. ² In Kentucky, for

¹ For an overview of hazmat regulations - Federal (DOT) <http://www.fmcsa.dot.gov/safety-security/hazmat/complyhregs.htm> & State (California) http://www.dmv.ca.gov/pubs/cdl_hm/sec9_a.htm

² Military munitions and certain radioactive and sensitive materials are exceptions. The federal government tracks these shipments using commercial satellite/GPS truck monitoring systems. For example, the Defense Transportation Tracking System (DTTS) monitors more than 47,000 arms, ammunition, and explosive shipments by commercial motor carriers each year in the continental

There are over **800,000 hazmat shipments per day** over the nation's highways including 75,000 shipments by tanker trucks.



DOT regulates all hazmat shipments, however, DOT & EPA co-regulate hazardous waste shipments.



Terrorists can use hazmat shipments as weapons of mass destruction. Securing hazmat shipments is an important DHS objective.

Government officials have almost no visibility into hazmat movement over the roads even though the technology for real-time tracking is commercially available & cost-effective.



EPA rules will allow companies to use electronic manifests for "cradle to grave" tracking of hazardous waste shipments.

EPA and DOT have different regulatory paradigms. EPA is concerned about illegal waste disposal and is focused on maintaining chain of custody control over waste shipments. DOT is concerned about shipment safety and security.

Hazardous waste and hazmat regulatory programs are State delegated programs.

example, state officials have almost no visibility into the movement of hazardous materials over the roads even though three major interstate corridors cut through the Commonwealth. The technology that would allow government agencies to track hazmat shipments on a real-time basis is commercially available and cost-effective, but federal/state regulatory programs are not sufficiently evolved to spur on its deployment.

Hazardous waste is a **subset** of the much larger hazardous materials (hazmat) universe. United States **Environmental Protection Agency** (EPA) regulations require companies to track the movement of hazardous waste from the point of generation to the point of disposal ("cradle to grave") using a hazardous waste manifest form. There are about four million hazardous waste shipments in the United States each year.

The manifest form is a shipping paper/bill of lading tailored to meet the needs of the hazardous waste regulatory business process. It must accompany all waste shipments. The parties to the waste shipment (generators, transporters, receiving facilities) apply their signatures to the manifest form as custody of the waste shipment changes hands. Currently, companies must use a multi-part paper manifest form. The use of paper manifests is cumbersome and expensive, and EPA plans to issue regulations that will allow companies to use electronic manifests (e-manifests) instead of paper manifests for hazardous waste shipments. EPA regulations governing hazardous waste shipments are described in **Appendix A**.

EPA and DOT share regulation of hazardous waste shipments and DOT accepts EPA's hazardous waste manifest form in satisfaction of its shipping paper requirement (note: EPA's regulatory role does not extend to the hazmat universe beyond hazardous waste). While there is some regulatory overlap between DOT and EPA, it is important to note that the two agencies operate off very different regulatory paradigms. DOT's hazmat regulatory focus is on maintaining the *safety and security* of hazmat shipments while EPA's regulatory focus is on maintaining waste shipment *chain of custody* to prevent illegal disposal. DOT places most of the responsibility for meeting its regulatory requirements on the hazmat carrier while EPA places most of its regulatory emphasis on the waste generator. Under EPA's regulatory view, a transporter is a passive party chosen by the generator to move waste from the generator to the generator's designated waste management facility. The generator retains full responsibility for ensuring that the waste shipment reaches its destination and is disposed of properly (e.g. full "cradle to grave" responsibility).

Since 9/11, DOT has increasingly emphasized the homeland security aspects of its hazmat transportation mission. EPA has not, however, expanded its regulatory focus even as it has worked on developing its e-manifest regulations. EPA views its e-manifest initiative primarily as a paperwork burden initiative and has not, to date, viewed its e-manifest program in the context of the nation's homeland security program.

The federal hazardous waste and hazmat programs are implemented in partnership with the States. In fact, the responsibility for managing hazardous waste and hazmat regulatory programs in the U.S. has been largely delegated to the States by the federal government. EPA/DOT issue federal regulations and provide funding for State programs. The States develop their own regulations which must be at least as stringent as EPA/DOT federal regulations. In Kentucky, the Environment and Public Protection Cabinet manages the hazardous waste regulatory program in lieu of EPA and develops the hazardous waste regulations that Kentucky companies follow. The Transportation Cabinet and the Justice and Public Safety Cabinet manage the hazmat regulatory program in lieu of DOT and develop State hazmat regulations and driver licensing programs.

United States. DTTS continuously monitors in-transit status of these shipments, providing GPS-derived location reports and coordinating emergency response efforts for accidents and other incidents.

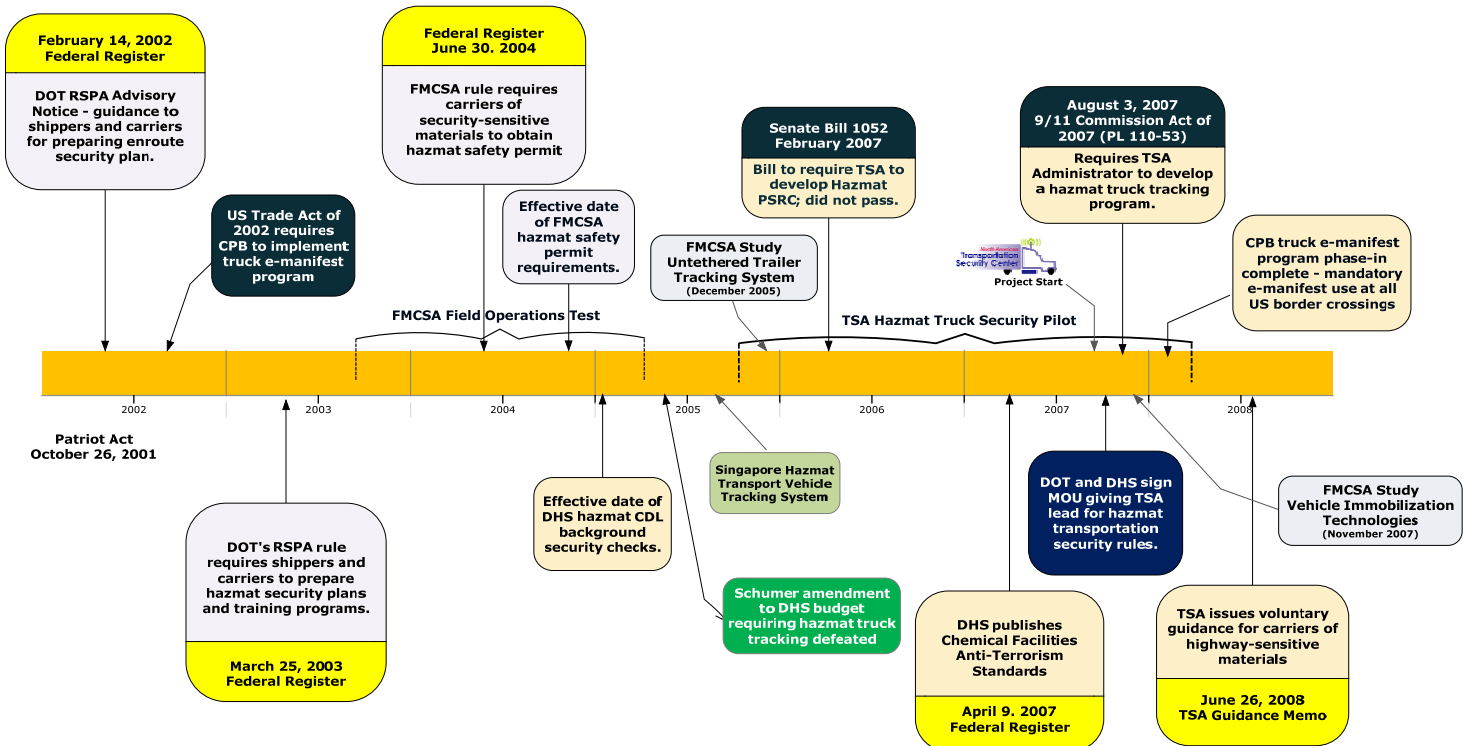
2.2 Hazmat security is driving the development of new regulations.

The government's focus on hazmat transportation has widened since 9/11. Prior to 9/11, the regulatory and legislative primary focus was on hazmat shipment safety. But since 9/11, the federal government has pursued an expanded regulatory and legislative agenda that recognizes the need to protect the hazmat supply chain from terrorists.

Since 9/11, the government's regulatory emphasis for hazmat shipments has shifted from safety to security.

Figure 2.2.a presents a timeline of regulatory and legislative developments that affect hazmat shipment security. Sections 2.2 - 2.5 discuss the implications of these developments on the design and operation of the North American Transportation Security Center.

Figure 2.2.a Timeline - Hazmat Security Regulations and Legislation



2.2.1 Shippers and carriers of certain hazardous materials must prepare security plans and conduct security training (RSPA/PHMSA).

On March 25, 2003, DOT's **Research and Special Programs Administration (RSPA)** established requirements to enhance the security of hazmat shipments (HM-232; 49 CFR 172.8).^{3 4} Under HM-232, hazmat shippers and carriers of certain hazardous materials must develop and implement security plans. In addition, HM-232 requires shippers and carriers to include a hazmat security component in their training programs.

HM-232 applies to all shippers and carriers who offer for transportation or transport the following types and quantities of hazardous materials:

- a hazardous material in an amount that must be placarded in accordance with Subpart F (Part 172) of DOT's hazardous materials regulations; or

Shippers and carriers of certain hazardous materials must prepare and follow written security plans including plans for en-route shipments.

³ <http://www.myregs.com/beginners/hm-232.pdf>

⁴ DOT created the Pipeline and Hazardous Materials Safety Administration (PHMSA) in February 2005. Hazmat transportation safety responsibilities shifted from the Research and Special Programs Administration to the PHMSA upon its creation.

- a hazardous material in a bulk packaging having a capacity equal to or greater than 13,248 L (3,500 gallons) for liquids or gases or more than 13.24 cubic meters (468 cubic feet) for solids; or
- a select agent or toxin regulated by the Centers for Disease Control and Prevention under 42 CFR Part 73; or
- a highway route-controlled quantity of a Class 7 (radioactive) material; or
- more than 25 kg (55 pounds) of a Division 1.1, 1.2, or 1.3 (explosive) material; or
- more than one L (1.06 qt) per package of a material poisonous by inhalation that meets the criteria for Hazard Zone A; or
- a shipment in other than a bulk packaging of 2,268 kg (5,000 pounds) gross weight or more of one class of hazardous materials amount that must be placarded in accordance with subpart F.

Shippers and carriers subject to HM-232 must develop and implement written security plans. In developing these plans, they must conduct risk assessments on their operations and develop security measures to address personnel security, facility security, and en route security. A security plan must include an assessment of possible transportation security risks for shipments and appropriate measures to address the assessed risks. At a minimum, a security plan must include the following three elements:

- personnel security - measures to confirm information provided by job applicants hired for positions that involve access to and handling of the hazardous materials covered by the security plan;
- unauthorized access - measures to address the possibility that unauthorized persons may gain access to the hazardous materials covered by the security plan or to transport conveyances being prepared for transportation of the hazardous materials covered by the security plan; and
- en-route security - measures to address the security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored incidental to movement.

Shippers and carriers must also provide hazmat employees with in-depth training on their security plan and its implementation. This training must include company security objectives, specific security procedures, employee responsibilities, actions to take in the event of a security breach, and the organizational security structure.

The FMCSA published an on-line hazmat security plan guidance for hazmat shippers and carriers.⁵ In addition, the RSPA published an **Advisory Notice** in the *Federal Register* to help shippers and carriers prepare en route security plans.⁶ RSPA's Advisory Notice was published in advance of its formal rulemaking. **Figure 2.2.b** is the en-route security advice that RSPA offered hazmat shippers.

It is important to note that both the shipper and carrier must prepare security plans under HM-232. However, a shipper is not required to determine if a carrier's security plan meets the requirements of HM-232. DOT advises shippers to work with their carriers to address en route security issues for the hazardous materials the carrier will be hauling on behalf of the shipper. In some cases, the shipper and carrier might develop a joint plan. In others, the shipper and carrier might have separate plans. However, a shipper's security plan should indicate the measures the shipper has taken

Hazmat security starts with security programs in place at the shipper's location.

RSPA's security guidance for hazmat shippers recommends use of vehicle tracking systems and crisis communications systems.

⁵Guide To Developing An Effective Security Plan For The Highway Transportation Of Hazardous Materials <http://www.fmcsa.dot.gov/safety-security/hazmat/security-plan-guide.htm>

⁶ Advisory Notices do have not regulatory force. They are for guidance purposes only. *Enhancing the Security of Hazardous Materials in Transportation*; Federal Register: February 14, 2002 (Volume 67, Number 31); Page 6963-6966; Research and Special Programs Administration DOT; RSPA-2002-11270, **Notice** No. 02-4; http://hazmat.dot.gov/regs/notices/misc/2002_11270_4.htm

to address en route security, such as coordination with the carrier to determine that the shipper's security plan covers en route security risks associated with the shipment.

Figure 2.2.b DOT's En-Route Security Guidance for Hazmat Shippers

Shippers and carriers can work together to assure the security of hazardous materials shipments en route from origin to destination:

Shippers should assess the transportation modes or combinations of modes available for transporting specific materials and select the most appropriate method of transportation to assure efficient and secure movement of product from origin to destination.

Know your carriers. Have a system for qualifying the carriers used to transport hazardous materials. Use carrier safety ratings, assessments, safety surveys, or audits and ask the carrier to provide information on security measures it has implemented. Verify the carrier has an appropriate employee hiring and review process, including background checks, and an on-going security training program.

Verify the identity of carrier and/or driver prior to loading a hazardous material. Ask the driver for photo identification and commercial driver's license and compare with information provided by the carrier. Ask the driver to tell you the name of the consignee and the destination for the material and confirm with your records before releasing shipments.

Identify preferred and alternative routing, including acceptable deviations. Strive to minimize product exposures to communities or populated areas, including downtown areas; avoid tunnels and bridges where possible; and expedite transportation of the shipment to its final destination.

Minimize stops en route; if you must stop, select locations with adequate lighting on well-traveled roads and check your vehicle after each stop to make sure nothing has been tampered with.

Consider using two drivers or driver relays to minimize stops during the trip. Avoid layovers, particularly for high hazard materials.

If materials must be stored during transportation, make sure they are stored in secure facilities.

Train drivers in how to avoid highjacking or stolen cargo--keep vehicles locked when parked and avoid casual conversations with strangers about cargoes and routes.

Consider if a guard or escort for a specific shipment or hazardous material is appropriate.

Consider utilizing advanced technology to track or protect shipments en route to their destinations. For example, you may wish to install tractor and trailer anti-theft devices or utilize satellite tracking or surveillance systems. As an alternative, consider frequent checks with drivers by cell phone to ensure everything is in order.

Install tamper-proof seals on all valves and package or container openings.

Establish a communication system with transport vehicles and operators, including a crisis communication system with primary and back-up means of communication among the shipper, carrier, and law enforcement and emergency response officials.

Implement a system for a customer to alert the shipper if a hazardous materials shipment is not received when expected. When products are delivered, check the carrier's identity with shipping documents provided by the shipper.

Get to know your customers and their hazardous materials programs. If you suspect you shipped or delivered a hazardous material to someone who may intend to use it for a criminal purpose, notify your local FBI office or local law enforcement officials.

Report any suspicious incidents or individuals to your local FBI office and to local law enforcement officials.

The requirements of HM-232 are particularly important to the chemical industry. Under the Responsible Care® program, chemical companies have banded together to develop standards and best management practices to help member companies meet their environmental, health, and safety responsibilities. **Figure 2.2.c** summarizes the relationship of HM-232 to the practices and standards developed under the Responsible Care® program.



The chemical industry has incorporated HM-232 requirements into its Responsible Care® program.

Figure 2.2.c illustrates the degree to which the chemical industry has internalized hazmat security programs for off-site shipments of hazardous materials. Additional requirements for enhanced hazmat security control of off-site hazmat shipments will not be unexpected by industry, and should not be uncomfortable from a compliance perspective.

Figure 2.2.c Relationship between HM-232 and the chemical industry's Responsible Care® program.

RSPA HM-232 Rule Requirements	Responsible Care® Security Management Practice	Responsible Care® Implementation and Compliance Tools
<p>Develop and adhere to a security plan. Components of the plan include: risk assessment; methods for confirming information provided by job applicants; measures to address the possibility of unauthorized persons that may attempt to gain access to hazmat or hazmat vehicles being prepared for transportation; and en route security.</p> <p>Plans should be in writing, retained, available to employees, and updated as needed.</p>	<p>Management Practice 1: Leadership Commitment</p> <p>Management Practice 2: Analysis of Threats and Vulnerabilities and Consequences</p> <p>Management Practice 3: Implementation of Security Measures</p> <p>Management Practice 5: Documentation</p> <p>Management Practice 8: Response to Security Threats</p> <p>Management Practice 12: Management of Change</p> <p>Management Practice 13: Continuous Improvement</p>	<p>Implementation Resource Guide for Responsible Care Security Code of Management Practices for Value Chain Activities (www.rctoolkit.com/security):</p> <p>Appendix 5: Value Chain Security Procedure/Plan Overview</p> <p>Appendix 3: Value Chain Security Risk Assessment Methodology</p> <p>Appendix 4: Examples of Security Measures</p> <p>RSPA Advisory Notice Issued on February 14, 2002, "Enhancing the Security of Hazardous Materials in Transportation" (http://hazmat.dot.gov/regs/notices/misc/2002_11270_4.htm)</p>
<p>Each hazmat employee must be trained on the plan and its implementation including company security objectives, specific procedures, responsibilities, actions in the event of a security breach, and organizational security structure</p>	<p>Management Practice 6: Training, Drills, and Guidance</p> <p>Management Practice 7: Communications, Dialogue and Information Exchange</p> <p>Management Practice 8: Response to Security Threats</p> <p>Management Practice 9: Response to Security Incidents</p>	<p>TRANSCAER® (Transportation Community Awareness and Emergency Response) (http://www.transcaer.org/downloads/resources/CommunityGuide.pdf)</p> <p>Implementation Resource Guide for Responsible Care Security Code of Management Practices for Value Chain Activities: Appendix 6: Examples of Security "Red Flags" (www.rctoolkit.com/security):</p> <p>CHEMTREC® (Chemical Transportation Emergency Center) (www.chemtrec.com) Chemical Sector ISAC (http://chemicalisac.chemtrec.com)</p>
<p>Security awareness training should be provided to all hazmat employees. Training should include awareness of security risk, methods designed to enhance transportation security, and how to recognize and respond to possible security threats.</p>	<p>Management Practice 3: Implementation of Security Measures</p> <p>Management Practice 6: Training, Drills, and Guidance</p> <p>Management Practice 8: Response to Security Threats</p> <p>Management Practice 9: Response to Security Incidents</p>	<p>The Department of Transportation's "HAZMAT Transportation Security Awareness Training Module" (hazmat.dot.gov/hmt_security.htm.)</p> <p>Implementation Resource Guide for Responsible Care Security Code of Management Practices for Value Chain Activities Appendix 6: Examples of Security "Red Flags" (www.rctoolkit.com/security):</p> <p>Chemical Sector ISAC (http://chemicalisac.chemtrec.com/)</p>

Since 1992, drivers of commercial motor vehicles have been required to obtain a commercial driver's license (CDL). Drivers hauling hazardous materials have to obtain an additional endorsement on their CDL.

2.2.2 States must perform security checks before licensing hazmat drivers.

Drivers have been required to have a commercial driver's license (CDL) in order to drive a commercial motor vehicle (CMV) since April 1, 1992. The **U.S. Federal Highway Administration** (FHWA) has developed and issued standards for testing and licensing CMV drivers. Among other things, the standards require States to issue CDLs to their CMV drivers only after the driver passes knowledge and skills tests administered by the State related to the type of vehicle to be operated. Drivers need CDLs if they are in

interstate, intrastate, or foreign commerce and drive a vehicle that meets one of the following definitions of a CMV:

- Class A -- Any combination of vehicles with a GVWR of 26,001 or more pounds provided the GVWR of the vehicle(s) being towed is in excess of 10,000 pounds.
- Class B -- Any single vehicle with a GVWR of 26,001 or more pounds, or any such vehicle towing a vehicle not in excess of 10,000 pounds GVWR.
- Class C -- Any single vehicle, or combination of vehicles, that does not meet the definition of Class A or Class B, but is either designed to transport 16 or more passengers, including the driver, or is placarded for hazardous materials.

Drivers who operate special types of CMVs also need to pass additional tests to obtain any of the following endorsements on their CDL:

- T - Double/Triple Trailers (Knowledge test only)
- P - Passenger (Knowledge and Skills Tests)
- N - Tank Vehicle (Knowledge Test only)
- **H - Hazardous Materials** (Knowledge Test only)
- X - Combination of Tank Vehicle and Hazardous Materials

Since January 2005 commercial truck drivers who want to renew or transfer their licenses to transport hazardous materials have undergone mandatory fingerprint and background checks, under a rule implemented by the **U.S. Transportation Security Administration (TSA)**.⁷

TSA implemented the program to meet the requirements of Section 1012 of the **USA Patriot Act** (October 2001), which prohibits states from issuing a commercial drivers license (CDL) to individuals to transport hazardous materials in commerce unless a determination has been made that the driver does not pose a security risk. Fees are collected from hazmat CDL applicants to cover the cost of background checks.

TSA estimates there are about 2.7 million truckers licensed to carry hazardous materials in the U.S. In January, Truckers must renew licenses to carry hazardous materials at least once every five years, although a state may require more frequent renewals. If TSA disqualifies an applicant, the driver can appeal the finding or seek a waiver from the agency.

2.2.3 Carriers of security-sensitive hazardous materials must obtain a hazmat safety permit (FMCSA).

Beginning January 2005, Federal Motor Carrier Administration regulations require carriers of the following security-sensitive hazardous materials to obtain a hazmat safety permit (Section 385.403).⁸

1. **Radioactive Materials:** A highway route-controlled quantity of Class 7 material, as defined in 173.403 of 49 CFR.
2. **Explosives:** More than 25kg (55 pounds) of a Division 1.1, 1.2 or 1.3 material, or an amount of a Division 1.5 material requiring a placard under Part 172 Subpart F of 49 CFR.

1. HAZMAT Endorsement Threat Assessment Program – United States Transportation Security Administration http://www.tsa.dhs.gov/what_we_do/layers/hazmat/index.shtml

⁸ Federal Motor Carrier Safety Regulations: Hazardous Materials Safety Permits; Final rule (69 FR 39350); June 30, 2004 49 CFR Parts 385, 386, and 390 [View PDF File](#)

Hazardous Materials Safety Permits; Supplemental Notice of Proposed Rulemaking (SNPRM); August 19, 2003 49 CFR Parts 385, 390, and 397 [View PDF File](#)



Since January 2005, TSA rules have required states to conduct security background checks on drivers before they are issued state licenses to haul hazardous materials.



FMCSA requires carriers of security-sensitive shipments to obtain hazmat safety permits.

3. **Toxic by Inhalation Materials:**

- *Hazard Zone A:* More than one liter (1.08 quarts) per package of a "material poisonous by inhalation," as defined in 171.8 of 49 CFR, that meets the criteria for "hazard zone A," as specified in 173.116(a) or 173.133(a) of 49 CFR.
 - *Hazard Zone B:* A "material poisonous by inhalation," as defined in 171.8 of this title, that meets the criteria for "hazard zone B," as specified in 173.116(a) or 173.133(a) of 49 CFR in a bulk packaging (capacity greater than 450 L [119 gallons]).
 - *Hazard Zone C & D:* A "material poisonous by inhalation," as defined in 171.8 of this title, that meets the criteria for "hazard zone C," or "hazard zone D," as specified in 173.116(a) of this title, in a packaging having a capacity equal to or greater than 13,248 L (3,500 gallons).
4. **Methane:** A shipment of compressed or refrigerated liquefied methane or liquefied natural gas or other liquefied gas with a methane content of at least 85% in a bulk packaging having a capacity equal to or greater than 13,248 L (3,500 gallons) for liquids or gases.

Hazmat safety permits focus on both safety and security performance of hazmat carriers.

To obtain a hazmat safety permit, a carrier must have a "satisfactory" safety rating. FMCSA will not issue a hazmat safety permit to a carrier that:

- does not certify that it has a satisfactory security program as required in Sec. 385.407(b); or
- has a crash rate in the top 30 percent of the national average as indicated in the FMCSA Motor Carrier Management Information System (MCMIS); or
- has a driver, vehicle, hazardous materials, or total out-of-service rate in the top 30 percent of the national average as indicated in the MCMIS.

In addition, a motor carrier must certify that it has a satisfactory security program to obtain a hazmat safety permit. The carrier must certify that it has:

- a security plan meeting the requirements of part 172, subpart I that addresses how the carrier will ensure the security of the written route plan required by this part; and
- a communications plan that allows for contact between the commercial motor vehicle operator and the motor carrier to meet the periodic contact requirements in Sec. 385.415(c)(1); and
- successful completion by all hazmat employees of the security training required in Sec. 172.704(a)(4) and (a)(5) of this title; and
- registration with the Research and Special Programs Administration (RSPA). The motor carrier must be registered with RSPA in accordance with part 107, subpart G.

There are a number of operational requirements that hazmat carriers must meet to obtain and keep a hazmat safety permit. Carriers are required to:

- maintain a "satisfactory" safety rating in order to obtain and hold a safety permit;
- maintain their crash rating, and their driver, vehicle, hazardous materials or out-of-service rating so they are not in the worse 30 percent of the national average as indicated in FMCSA's Motor Carrier Management Information System (MCMIS);
- have a satisfactory security program (and associated training) according to 49 CFR 173.800 in place;
- maintain registration with RSPA;
- develop a system of communication that will enable the vehicle operator to contact the motor carrier during the course of transportation and maintain records of these communications (Section 385.415);
- have written route plan required for radioactive materials set forth in 49 CFR 397.101 and for explosives in Part 397.19 (currently required); and
- perform a pre-trip inspection (North American Standard (NAS) Level VI Inspection Program for Radioactive Shipments) for shipments containing highway route controlled Class 7 (radioactive) materials.

Carriers have to maintain frequent contact with drivers and keep records of contact made. FMCSA recognizes wireless GPS systems as satisfying communications requirements.

The communications requirements of Section 385.415 are notable. The FMCSA has specifically recognized that an electronic GPS tracking system or other periodic wireless tracking system will fulfill the communications requirements of Section 385.415. However, the carrier (or driver) must keep a record of communications with the necessary information (date, time, location, driver's name, truck ID). These records can be kept electronically. The information may be stored in separate databases, as long as the information can be correlated at the request of an official in a timely manner.

The FMCSA estimates that about 3,100 carriers will be covered by its hazmat security regulations.

Figure 2.2.d Number of carriers requiring FMCSA hazmat safety permits.

Carriers	Number of small carriers	Total carriers
Total Number of Carriers for List of Materials Covered	2,436	3,131
Number of Interstate Carriers	1,664	2,139
Number of Intrastate Carriers	772	992

About 3,100 hazmat carriers will receive hazmat safety permits. Maintaining communications records represents almost the entire compliance cost for hazmat carriers.

According to the FMCSA, the major driver of hazmat carrier costs is the cost to record and maintain communication records. This cost item represents about 99 percent of the total annual costs to hazmat carriers to comply with the permit program requirements.

2.2.4 Chemical facility anti-terrorism standards focus on hazmat security (DHS).

The FMCSA study acknowledged the implementation problem of industry-led voluntary programs by suggesting that "government intervention" (e.g. regulations) might be needed. The argument for "government intervention" is buttressed by DHS's experience in its efforts to beef up security at chemical production plants in urban areas. In that case, an industry-led voluntary initiative to upgrade chemical plant security resulted in such a tepid industry response that DHS sought legislation authorizing DHS to develop and implement a framework to regulate the security of high-risk chemical facilities in the United States.⁹

In October 2006, the President signed the Department of Homeland Security Appropriations Act of 2007, which in Section 550 authorized DHS to require high-risk chemical facilities to complete security vulnerability assessments, develop site security plans, and implement risk-based measures designed to satisfy DHS-defined risk-based performance standards. The Act also authorized DHS to enforce compliance with the security regulations, including conducting audits and inspections of high-risk facilities, imposing civil penalties of up to \$25,000 per day, and shutting down facilities that fail to comply with the regulations.¹⁰

DHS's Chemical Facility Anti-Terrorism Standards focus on the security of chemicals (hazardous materials) made or stored at chemical facilities.

DHS published an Interim Final Rule (IFR), the **Chemical Facility Anti-Terrorism Standards (CFATS)**, on April 9, 2007. The rules contain a list of 300 chemicals (called Appendix A), and any facility which stores an Appendix A chemical in greater than a threshold quantity (also listed on Appendix A) is considered a chemical facility. A chemical facility that possesses a chemical of interest at or above the screening threshold quantity (STQ) must complete and submit an assessment called a Top-Screen assessment within 60 calendar days of coming into possession of the listed chemicals at or above the listed STQs.

DHS estimates the Top-Screen will take between thirty and forty hours to complete. The Top-Screen must be submitted by an officer of the corporation, or by someone designated by an officer, and that person must attest to the accuracy of the information.

After completing the Top-Screen, a facility may be notified to take further actions, including submission of a Security Vulnerability Assessment and a Site Security Plan.

⁹ Chemical and Engineering News; *Chertoff Calls for Legislation: DHS Secretary Wants Federal Regulation of Chemical Industry Security*; March 27, 2006 <http://pubs.acs.org/cen/news/84/i13/8413notw1.html>

¹⁰ DHS Critical Infrastructure: Chemical Security webpage http://www.dhs.gov/xprevprot/programs/gc_1169501486179.shtm

Chemical facilities may be subject to inspection by DHS officials. Inspectors may review records, take photographs, and talk with employees.

Unlike EPA inspections, the information DHS obtains is placed in a confidential file and is not subject to FOIA requests from the public. However, there is some overlap between the CFATS rules and the Tier Two Hazardous Chemical Inventories which are provided to state and local governments and with the hazard communication program required by the Occupational Safety and Health Administration (OSHA). Also, Appendix A contains different chemicals and different thresholds than the U.S. Environmental Protection Agency (EPA) and OSHA requirements.

For each Appendix A chemical, DHS justifies its inclusion on the list based on a number of factors including:

Release, Theft, or Sabotage Potential	Security Issue
<ul style="list-style-type: none"> o Minimum Concentration (%) o Screening Threshold Quantities (pounds) 	<ul style="list-style-type: none"> o Release – Toxic o Release – Flammable o Theft – chemical weapons or chemical weapons precursor o Theft – weapons of mass effect o Theft – explosives or improvised explosive device precursor o Sabotage or Contamination

2.3 In 2007, TSA assumed the lead federal responsibility for hazmat transportation security rulemaking.

DOT's Pipeline and Hazardous Materials Administration (PHMSA) published a notice in the *Federal Register* on **June 27, 2007** advising that the Transportation Security Administration has assumed the lead role from PHMSA for rulemaking addressing the security of motor carrier shipments of hazardous materials.

The action was consistent with and supportive of the respective transportation security roles and responsibilities of the Department of Transportation and DHS as delineated in a Memorandum of Understanding (MOU) signed September 28, 2004, and of TSA and PHMSA as outlined in an Annex to that MOU signed August 7, 2006.

The PHMSA also used the *Federal Register* notice to withdraw an Advanced Notice of Proposed Rulemaking (ANPRM) related to hazmat transportation security that the PHMSA had published on July 16, 2002. The ANPRM solicited comments on a variety of security measures that might be required of hazmat carriers to improve hazmat supply chain security including the use of vehicle tracking and monitoring systems, emergency warning systems, and remote shut-offs. Follow-up action to the ANPRM had been put on hold in light of the FMCSA's Field Operations Test (refer to Section 4.1 of this report) and TSA's Hazmat Truck Security Pilot (refer to Section 4.2 of this report) as well as the shifting responsibilities of DOT and DHS.

With this *Federal Register* notice, TSA will be responsible for all future security regulations for hazmat motor carriers.

2.4 TSA issued guidance for shippers and carriers of highway security-sensitive materials on June 26, 2008.

Almost one year to the day that TSA formally assumed the lead federal responsibility for hazmat transportation security regulations, TSA issued guidance for shippers and carriers of highway security-sensitive materials. The guidance was issued by TSA's Assistant Administrator for Transportation Sector Network Management on June 26, 2008.¹¹ TSA's guidance recognizes two tiers of highway security-sensitive materials.



TSA has the lead responsibility for hazmat transportation security rulemaking.

¹¹ Letter to Highway and Motor Carrier Stakeholders; John P. Sammon, Assistant Administrator, Transportation Sector Network Management, US Transportation Security Administration; June 26, 2008.

1. **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. A full list of Tier 1 HSSM may be found in **Appendix B**.
2. **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. A full list of Tier 2 HSSM may be found in **Appendix B**.



TSA's highway security-sensitive security guidance recognizes two classes of highway security-sensitive materials:

- Tier 1 which can cause highly significant adverse effects from terrorist actions; and
- Tier 2 which can cause moderately significant adverse effects from terrorist actions.

2.4.1 TSA's security recommendations incorporate/enhance earlier DOT guidance.

TSA developed its guidance in conjunction with other Federal agencies including DOT's Pipeline and Hazardous Material Safety Administration (PHMSA) and DOT's Federal Motor Carrier Safety Administration. The TSA guidance builds upon existing PHMSA and FMCSA hazmat regulations including PHMSA's hazmat safety regulatory provisions in 49CFR172.704 and 172.800 that require hazmat carriers to develop and implement security programs and to train employees in security matters. TSA has, however, enhanced earlier guidance to strengthen en-route security measures for shippers and carriers of high-risk materials.

TSA's guidance is not mandatory for hazmat shippers and receivers. Shippers and carriers are, however, advised by TSA to implement security programs consistent with TSA June 26th guidance.

2.4.2 TSA recommends more stringent security measures for Tier 1 highway security-sensitive materials.

As illustrated in **Figure 2.4.a**, TSA listed 23 Security Action Items (SAI) in its June 26th guidance. The SAIs were divided into four categories 1). general security; 2). personnel security; 3). unauthorized access; and 4). en-route security.

TSA recommends that shippers and carriers of Tier 2 HSSMs adopt the first sixteen SAIs and that shippers and carriers of **Tier 1 HSSMs, the riskiest materials from a security perspective, adopt the first sixteen SAIs as well as TSA's security action items 17-23**. A discussion of TSA's security action items 17-23 follows.

SAIs 17-23 apply only to Tier 1 HSSM shipments.

Figure 2.4.a TSA HSSM Security Action Items

TSA HSSM Security Action Items	
<p>General Security:</p> <ol style="list-style-type: none"> 1. Security Assessment and Security Plan Requirements. 2. Awareness of Industry Security Practices. 3. Inventory Control Process. 4. Business and Security Critical Information <p>Personnel Security:</p> <ol style="list-style-type: none"> 5. Possession of a Valid Commercial Drivers License - Hazardous Materials Endorsement. 6. Background Checks for Highway Transportation Sector Hazmat Employees other than Motor Vehicle Drivers with a Valid CDL with HME. 7. Security Awareness Training for Hazmat Employees. <p>Unauthorized Access:</p> <ol style="list-style-type: none"> 8. Access Control System for Drivers. 9. Access Control System for Facilities Incidental to Transport. 	<p>En-Route Security:</p> <ol style="list-style-type: none"> 10. Establish Communications Plan. 11. Establish Appropriate Vehicle Security Program. 12. Establish Appropriate Cargo Security Program. 13. Implement a Seal/Lock Control Program. 14. High Alert Level Protocols. 15. Establish Security Inspection Policy and Procedures. 16. Establish Reporting Policy and Procedures. 17. Shipment Pre-Planning, Advance Notice of Arrival, and Receipt of Confirmation Procedures. 18. Preplanning Routes. 19. Security for Trips Exceeding Driver Hours of Service. 20. Dedicated Truck. 21. Tractor Activation Capability. 22. Panic Button Capability. 23. Tractor and Trailer Tracking Systems

SAI #17 calls for close coordination between shipper and receiver including establishment of communication systems to establish ETA and to track delivery schedules.

SAI #18 suggests shippers and carriers establish primary and alternate routes. Carriers should avoid highly populated urban areas or critical infrastructure during Orange or Red alerts.

SAI #19 suggests carriers take security precautions when trips are interrupted so that drivers meet hours of service requirements.

SAI #20 suggests that Tier 1 shipments not be subcontracted or transloaded unless the subcontractor is security cleared.

SAI #21 suggests that carriers use in-cab devices that require drivers to log-in to drive the tractor. **SAI #22** suggests that drivers have access to a panic button (in-cab and/or remote).

Security Action Item #17. Shipment Pre-Planning, Advance Notice of Arrival and Receipt Confirmation Procedures with Receiving Facility – 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.

Security Action Item #18. Preplanning Routes – 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 en-route deviation is necessary.

Security Action Item #19. Security for Trips Exceeding Driving Time under the Hours of Service of Drivers Regulation (49 CFR Part 395) – 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

Security Action Item #20. Dedicated Truck – 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.

Security Action Item #21. Tractor Activation Capability – 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.

Security Action Item #22. Panic Button Capability – 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.








Security Action Item #23. Tractor and Trailer Tracking Systems – 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. Geo-fencing 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

SAI #23 suggests the use of tractor **and** trailer tracking systems. Systems should allow for route adherence tracking and monitoring of trailer “connect” and “disconnect”.

Figure 2.4.b lists Tier 1 HSSMs and the number of annual U.S. shipments of each HSSM.


Figure 2.4.b TSA Tier 1 HSSMs

DOT Hazard Class	Hazmat Placard	Threshold Quantity	Number of Annual U.S. Shipments ¹²
Division 1.1 Division 1.2 Division 1.3 Explosives		Any quantity	Domestic - 11,868 NAFTA - 524
Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation)		Anhydrous ammonia (UN1005) in single bulk packaging >300 L or 3000 kg	Domestic - 563,771 ¹³ NAFTA - 6,767
Division 2.3 Toxic (Poison) Gas Division 2.3 Toxic (Poison) Gas		Hazard zone A & B >5lbs. in a single package Hazard zone C & D in single bulk packaging >3000L or 3000kg	Domestic - 960,871 NAFTA - 8,233
Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation)		PG I in single bulk packaging > 3000 L or 3000 kg	Domestic - 62,015,889 ¹⁴ NAFTA - 119,816
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)		Hazard zone A & B > 5 lbs. in a single package	Domestic - 307,244 NAFTA - 18,213
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)		Hazard zone C & D in single bulk packaging > 3000 l or 3000 kg	
Class 7 Radioactive Materials		IAEA Code of Conduct Category 1 and 2 materials including Highway Route Controlled quantities as defined in 49 CFR 173.403 or known as radionuclides in forms as RAM-QC by the Nuclear Regulatory Commission	Domestic - 7,777 NAFTA - 7,265

¹² Data on the number of Tier 1 HSSM shipments was provided by David Cooper, Program Manager, Highway & Motor Carrier Division, U.S. Transportation Security Administration. Data represents 2005 projections for US domestic and NAFTA truck traffic for select hazmat commodities.

¹³ This figure includes shipments of Tier 2 Division 2.2 Non-Flammable Gases (subsidiary hazard Oxidizer Division 5.1).

¹⁴ This figure includes shipments of : 1). Class 3 Flammable Liquids (PGI and II in single bulk packaging > 300L or 3000 kg; and 2). Class 3 Flammable Liquids (any quantity desensitized explosives) – both of which are Tier 2 HSSM.

Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation)		Packing group I and II in single bulk packaging > 3000 L or 3000 kg	Domestic - 4,548,595 ¹⁵ NAFTA - 95,703
Other Materials		Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules.	unknown
			Domestic - 1,287,760 ¹⁶ NAFTA - 34,235

2.5 The 9/11 Commission Act of 2007 (PL 110-53/H.R. 1) requires TSA to take action on hazmat shipment tracking.

On August 3, 2007, President Bush signed the "Implementing Recommendations of the 9/11 Commission Act of 2007". This comprehensive legislation consists of 24 Titles addressing a broad range of matters intended to enhance homeland security and counter the terrorist threat.



President Bush signed P.L. 110-53 on August 3, 2007. It includes provisions to enhance transportation security.

The Act is a consolidation of three former House and Senate bills – H.R. 1, which bore the title "Implementing the 9-11 Commission Recommendations Act of 2007"; S. 4, "Improving America's Security Act of 2007"; and H.R. 1401, "Rail and Public Transportation Security Act of 2007."

Subject areas covered in the Act include homeland security and emergency management performance grants; communications interoperability; strengthening use of the incident command system; improving intelligence and information sharing and Congressional oversight of intelligence; preventing terrorist travel; privacy and civil liberties; private sector preparedness; improving critical infrastructure security; enhanced defenses against weapons of mass destruction; **enhancing transportation security**; preventing weapons of mass destruction proliferation and terrorism; international cooperation on security technologies; 9/11 Commission international implementation; and advancing democratic values.

2.5.1 Earlier legislative initiatives paved the way for PL 110-53.

Use of smart truck technology is voluntary, but legislative & regulatory pressure for mandatory deployment is increasing.

To date, adoption of smart truck technology to protect hazmat shipments has been voluntary on the part of trucking fleets. And, many fleets – especially the larger, long-haul fleets – have extensive smart truck technology systems in place. For example, Qualcomm – a participant in the FMCSA smart truck technology study – has installed its commercial communications and position-reporting technology on more than 500,000 commercial vehicles. Qualcomm's customers include more than 1,500 trucking companies, and 34 of the top 35 truckload fleets. However, even with the commercial success of Qualcomm and others, the FMCSA study concluded that smart truck technology has not been deployed extensively enough in the hazmat supply chain and that the government security infrastructure is not sufficiently developed to provide the level of protection the country needs for hazmat shipments.

A number of regulatory/legislative initiatives have been undertaken by government agencies to accelerate the deployment of smart truck technology to protect hazmat shipments.

¹⁵ This figure includes shipments of Class 8 Corrosive Materials (Packing group I in single bulk packaging > 3000L or 3000kg) which is a Tier 2 HSSM.

¹⁶ This figure does not include Tier 1 Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation) or Tier 1 Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation) or Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation). Data is unavailable on the number of these shipments.

In 2004, the **State of California** considered legislation (AB 575) that would have required all California registered trucks engaged in the transportation of flammable and combustible liquids in cargo trucks to be equipped with a GPS system. The GPS system would enable the motor carrier to find the truck's location at any time. The legislation also required installation of remote vehicle shutdown (RVS) devices on all California-domiciled trucks carrying hazardous materials. The RVS devices had to be accessible to California Highway Patrol (CHP) officials so that CHP would be able to remotely disable a truck by activating the truck's RVS device. AB 575 was designed to give law enforcement and fleet owners more control of hazmat trucks in the event of a hijacking by a terrorist or a mentally unstable individual.



In 2004, California considered requiring all hazmat transporters to install GPS and remote vehicle shutdown devices on their trucks.

The bill had particularly strong support from California's law enforcement community – especially the California Highway Patrol. CHP's support of the bill was due, in part, to an incident that occurred in early 2001. In that incident, a driver slammed an 18-wheeler into California's state Capitol building. The driver – an ex-convict and mental patient – was killed in the crash. The truck was destroyed by fire and \$10million in damage was done to the Capitol building. According to CHP officials, had the truck been carrying a flammable or explosive substance, the entire Capitol building would have been destroyed. AB 575 passed easily in the state assembly but was sidetracked in the California senate in the face of opposition by the trucking industry which argued that it would place too much financial burden on hazmat transporters and that too little thought had been given to implementation, especially related to CHP access to RVS devices on the trucks. California legislators plan to reintroduce the bill in modified form in the future.

AB 575 was opposed by the trucking industry and was tabled in the California Senate.

The need to protect the hazmat supply chain has captured the attention of U.S. legislators. In the 108th Congress, the **United States Senate** considered an amendment introduced by Sen. Charles Schumer (D-N.Y.) to the Department of Homeland Security's appropriations bill that would have required:

Since 9/11 federal legislators have become concerned about the use of hazmat shipments as weapons of mass destruction.

1. trucks transporting hazardous materials to be equipped with global positioning satellite (GPS) tracking devices; and
2. written route plans to be prepared and filed with DHS prior to transporting hazardous materials.



Noting the growing preference of terrorists to use truck bombs in their attacks, Schumer remarked on the Senate floor,

In 2004, the U.S. Senate considered an amendment to the DHS appropriations bill requiring hazmat GPS tracking and written route plans.

...“You can buy a car and pay a couple hundred bucks more and have a GPS system which tells exactly where the vehicle is. Wouldn't it make sense that every truck carrying hazardous material was required to have such a GPS system? That would mean if the truck were stolen, if the truck were taken to a far different location than where it should be and the company wished to find out where it was, we could find it in a minute.”

Schumer's amendment drew opposition from the American Trucking Associations (ATA). The ATA criticized the measure as unnecessarily burdensome and characterized GPS-based tracking systems as expensive and “easily defeated.” Republicans and several farm state Democrats combined to defeat the measure. Sen. Thad Cochran (R-Mississippi), chairman of the Homeland Security Subcommittee of the Senate Appropriations Committee, argued that other measures were already in place to address hazmat security, including shipper training and Highway Watch® programs as well as a research effort by the Federal Motor Carrier Safety Administration to test and evaluate a variety of technologies, including GPS, for identifying potentially dangerous vehicles.

The amendment was opposed by the American Trucking Associations, and tabled in the U.S. Senate.

The Senate voted 55-34 to table the Schumer amendment, instead adopting a more modest proposal from Sen. Harry M. Reid (D-Nevada) that appropriated \$2 million to support efforts for identification and tracking of trucks carrying hazmat cargoes and \$53 million to continue and expand upon the background check system for commercial driver licenses with a hazmat endorsement.

In the October 2004 issue of *GPS World*, a leading trade magazine, the magazine's editor criticized ATA's opposition to GPS-based tracking systems for hazmat shipments



The trucking industry's motivation for resisting the amendment's hazmat GPS tracking requirement was motivated by "just not wanting to be obliged (by the government) to do something...."

...Clearly, GPS is not a complete solution for the security needs of the U.S. transportation system. But just as clearly GPS should be a part of that solution. It's past time to make it so."

Editor - *GPS World*
October 2004

U.S. Senate Bill 1052 would have authorized DHS/DOT to develop a hazmat PSRC; regulations would drive smart truck technology adoption.

as being disingenuous and short-sighted.¹⁷

"...Ironically, for years a rapidly growing number of trucking companies have been outfitting their fleets with just the kind of capability that ATA dismisses as an expensive, vulnerable, and cumbersome mandate, primarily because of the increased productivity that results.

Of course, this is not the first instance of an industry resisting a security mandate. After 9/11, commercial airlines resisted some suggestions for methods of increasing security against terrorists, or argued that the government should pay for these measures. The dissenters usually have some credible reasons for not complying with the directive. Privacy. Cost. Bureaucratic burden. Inadequate preparation time. But the unspoken motive often seems to come from just not wanting to be obliged to do something.

It brings to mind the closing stanza of Rudyard Kipling's poem, "The Lesson," composed in the wake of the disastrous Boer War: "We have forty million reasons for failure, but not a single excuse."

Clearly, GPS is not a complete solution for the security needs of the U.S. transportation system. But just as clearly GPS should be a part of that solution. It's past time to make it so. "

In the 109th Congress, Senate Bill 1052 – sponsored by Senator Ted Stevens (R-Alaska) and co-sponsored by Schumer and others – would have required the Secretary of Homeland Security and the Secretary of Transportation to develop a **National Public Sector Response System** patterned on the PSRC concept from the FMCSA hazmat security study. The bill was referred out of committee for debate by the full Senate on February 27, 2006 and has yet to be scheduled for full debate. Senate Bill 1052 failed to survive Senate debates, but it is notable in that it recognized the need for a Hazmat Public Sector Reporting Center and embraced the idea that a regulatory "push" – like that implemented in Singapore - is needed to promote smart truck technology deployment.

2.5.2 PL 110-53 requires TSA to develop a hazmat truck tracking program.



Transportation Security Administration

PL 110-53 requires TSA to develop a hazmat truck tracking program.

Section 1554 of PL 110-53 directs the Secretary of the Department of Homeland Security, through the TSA Administrator, to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides frequent or continuous communications, vehicle position location and tracking capabilities, and a feature that allows the driver to broadcast an emergency distress signal. The text of Section 1554 follows.

SECTION 1554. MOTOR CARRIER SECURITY-SENSITIVE MATERIAL TRACKING.

(a) Communications.--

(1) *In general.--Not later than 6 months after the date of enactment of this Act, consistent with the findings of the Transportation Security Administration's hazardous materials truck security pilot program, the Secretary, through the Administrator of the Transportation Security Administration and in consultation with the Secretary of Transportation, shall develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides--*

(A) frequent or continuous communications;

(B) vehicle position location and tracking capabilities; and

(C) a feature that allows a driver of such vehicles to broadcast an emergency distress signal.



PL 110-53 requires that TSA's truck tracking program be consistent with the findings of TSA's Hazmat Truck Security Pilot.

¹⁷ "Hazmat Keeps On Truckin'," October 1, 2004, GPS World <http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=126157>

(2) Considerations.--In developing the program required by paragraph (1), the Secretary shall--

(A) consult with the Secretary of Transportation to coordinate the program with any ongoing or planned efforts for motor carrier or security-sensitive materials tracking at the Department of Transportation;

(B) take into consideration the recommendations and findings of the report on the hazardous material safety and security operational field test released by the Federal Motor Carrier Safety Administration on November 11, 2004; and

(C) evaluate--

(i) any new information related to the costs and benefits of deploying, equipping, and utilizing tracking technology, including portable tracking technology, for motor carriers transporting security-sensitive materials not included in the hazardous material safety and security operational field test report released by the Federal Motor Carrier Safety Administration on November 11, 2004;

(ii) the ability of tracking technology to resist tampering and disabling;

(iii) the capability of tracking technology to collect, display, and store information regarding the movement of shipments of security-sensitive materials by commercial motor vehicles;

(iv) the appropriate range of contact intervals between the tracking technology and a commercial motor vehicle transporting security-sensitive materials;

(v) technology that allows the installation by a motor carrier of concealed electronic devices on commercial motor vehicles that can be activated by law enforcement authorities to disable the vehicle or alert emergency response resources to locate and recover security-sensitive materials in the event of loss or theft of such materials;

(vi) whether installation of the technology described in clause (v) should be incorporated into the program under paragraph (1);

(vii) the costs, benefits, and practicality of such technology described in clause (v) in the context of the overall benefit to national security, including commerce in transportation; and

(viii) other systems and information the Secretary determines appropriate.

(b) Funding.--From the amounts appropriated pursuant to section 114(w) of title 49, United States Code, as amended by section 1503 of this Act, there shall be made available to the Secretary to carry out this section--

(1) \$7,000,000 for fiscal year 2008 of which \$3,000,000 may be used for equipment;

(2) \$7,000,000 for fiscal year 2009 of which \$3,000,000 may be used for equipment; and

(3) \$7,000,000 for fiscal year 2010 of which \$3,000,000 may be used for equipment.

(c) Report.--Not later than 1 year after the issuance of regulations under subsection (a), the Secretary shall issue a report to the appropriate congressional committees on the program developed and evaluation carried out under this section.

(d) Limitation.--The Secretary may not mandate the installation or utilization of a technology described under this section without additional congressional authority provided after the date of enactment of this Act.

2.5.3 PL 110-53 requires DHS to evaluate hazmat truck routes.

Section 1553 of PL 110-53 directs the Secretary of the Department of Homeland Security to: (1) document existing and proposed routes for the transportation of hazardous materials by motor carrier; (2) assess and characterize such routes to identify measurable criteria for selecting routes based on safety and security concerns; (3) prepare guidance materials for state officials to assist them in identifying and reducing safety concerns and security risks when designating routes for hazardous materials; and (4) complete an assessment of the safety and national security benefits achieved under existing requirements for route plans for explosives and radioactive materials. The text of Section 1553 follows.

SEC. 1553. HAZARDOUS MATERIALS HIGHWAY ROUTING

(a) Route Plan Guidance.--Not later than 1 year after the date of enactment of this Act, the Secretary of Transportation, in consultation with the Secretary, shall--

The TSA hazmat truck tracking program must factor the **FMCSA Field Operations Test** results into its design (refer to Section 3.1).

The law requires TSA to consider a number of things including:

- cost/benefit of "smart truck" technology deployment;
- ability to resist tampering and disabling;
- contact intervals (polling rates); and
- vehicle immobilization.

PL 110-53 allocates \$7 million for the current fiscal year and \$7 million/year for the following two fiscal years to fund TSA's hazmat truck tracking program.



PL 110-53 requires DHS to evaluate truck transportation routes for radioactive and nonradioactive hazardous materials.

(1) document existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier, and develop a framework for using a geographic information system-based approach to characterize routes in the national hazardous materials route registry;

(2) assess and characterize existing and proposed routes for the transportation of radioactive and nonradioactive hazardous materials by motor carrier for the purpose of identifying measurable criteria for selecting routes based on safety and security concerns;

(3) analyze current route-related hazardous materials regulations in the United States, Canada, and Mexico to identify cross-border differences and conflicting regulations;

(4) document the safety and security concerns of the public, motor carriers, and State, local, territorial, and tribal governments about the highway routing of hazardous materials;

(5) prepare guidance materials for State officials to assist them in identifying and reducing both safety concerns and security risks when designating highway routes for hazardous materials consistent with the 13 safety-based nonradioactive materials routing criteria and radioactive materials routing criteria in subpart C part 397 of title 49, Code of Federal Regulations;¹⁸

(6) develop a tool that will enable State officials to examine potential routes for the highway transportation of hazardous materials, assess specific security risks associated with each route, and explore alternative mitigation measures; and

(7) transmit to the appropriate congressional committees a report on the actions taken to fulfill paragraphs (1) through (6) and any recommended changes to the routing requirements for the highway transportation of hazardous materials in part 397 of title 49, Code of Federal Regulations.

(b) Route Plans.--

(1) Assessment.--Not later than 1 year after the date of enactment of this Act, the Secretary of Transportation shall complete an assessment of the safety and national security benefits achieved under existing requirements for route plans, in written or electronic format, for explosives and radioactive materials. The assessment shall, at a minimum--

(A) compare the percentage of Department of Transportation recordable incidents and the severity of such incidents for shipments of explosives and radioactive materials for which such route plans are required with the percentage of recordable incidents and the severity of such incidents for shipments of explosives and radioactive materials not subject to such route plans; and

(B) quantify the security and safety benefits, feasibility, and costs of requiring each motor carrier that is required to have a hazardous material safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry such a route plan that meets the requirements of section 397.101 of that title when transporting the type and quantity of hazardous materials described in section 385.403, taking into account the various segments of the motor carrier industry, including tank truck, truckload and less than truckload carriers.

(2) Report.--Not later than 1 year after the date of enactment of this Act, the Secretary of Transportation shall submit a report to the appropriate congressional committees containing the findings and conclusions of the assessment.

PL 110-53 requires DHS to develop a tool that will enable State officials to examine potential hazmat routes and to assess security risks associated with each route.

Under PL 110-53 DOT must require motor carriers subject to FMCSA's hazardous material safety permitting requirements to maintain, follow, and carry a route plan in written or electronic format.

¹⁸ Refer to 49CFR 397.71. In establishing, maintaining, or enforcing a specific non-radioactive hazmat route, a state must consider the following federal standards: population density; type of highway; types and quantities of NRHM; emergency response capabilities; results of consultation with affected persons; exposure and other risk factors; terrain considerations; continuity of routes; alternative routes; effects on commerce; delays in transportation; climatic conditions; and congestion and accident history.

(c) Requirement.--The Secretary shall require motor carriers that have a hazardous material safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry a route plan, in written or electronic format, that meets the requirements of section 397.101 of that title when transporting the type and quantity of hazardous materials described in section 385.403 if the Secretary determines, under the assessment required in subsection (b), that such a requirement would enhance security and safety without imposing unreasonable costs or burdens upon motor carriers.



TSA's Hazmat Truck Security Pilot has proven that a hazmat tracking program is feasible. TSA believes the pilot program has established a solid foundation for implementing PL 110-53.

2.5.4 TSA plans to expand on its recently completed Hazmat Truck Security Pilot program.

PL 110-53 requires TSA to develop its hazmat tracking program to be consistent with the findings of TSA's Hazmat Truck Security Pilot. The TSA Hazmat Truck Security Pilot was completed April 2008 and is described in **Section 4.2** of this report. On February 25, 2008, the project team met with representatives of TSA's Transportation Sector Network Management Branch of the Highway Motor Carrier Programs Office. The project team was provided with a document describing TSA's high-level plan for implementing H.R. 1. It is included in this report as **Appendix C**.

In its plan for implementing H.R. 1, TSA stated that its Hazmat Truck Security Pilot demonstrates the feasibility of implementing a hazmat truck tracking program.

"The pilot project has shown that the transition from pilot to program is feasible. It has demonstrated a prototype for a centralized truck tracking center. The truck tracking center was used to coordinate incident response with appropriate first responders and a government intelligence operations center. The truck tracking center system collected data in real-time from carrier-operated systems utilized in the field. Upon receiving an alert notification or upon detection of an abnormal condition, truck tracking center dispatchers helped manage the process of notifying stakeholders and coordinating responses to transportation security incidents."

Furthermore, TSA pointed out in its plan that its Hazmat Truck Security Pilot established the foundation for satisfying the three general requirements of §1554(a)(1) of H.R. 1.

- **Frequent or continuous communications** – TSA has developed a set of tested protocols that are capable of interfacing with (a) existing truck tracking systems, (b) state/local law enforcement agencies and first responders and (c) with federal intelligence and emergency management centers.
- **Vehicle position location and tracking capabilities** – TSA has implemented a tested and functioning truck tracking center that allows TSA to "continually" monitor truck locations and track load types in all of the continental United States.
- **A feature that allows a driver of such vehicles to broadcast an emergency distress signal** – TSA has developed a concept of operations that has gone through considerable testing and being vetted by government and industry volunteers. This concept of operations facilitates effective responses to drivers' emergency distress signals.

TSA plans to take the following actions as a follow-up to the Hazmat Truck Security Pilot:

1. further develop its standards-based communications interface to adapt to evolving technical and functional requirements;
2. fully develop and implement a scalable truck tracking center to function as a central operations control area to (i) collect data from motor carriers, (ii) monitor events and coordinate a response, and (iii) facilitate communications to support a coordinated response; and
3. further refine the systems and algorithms that provide the foundation of truck tracking center system's risk-based approach to transportation event management.



TSA has prepared a high-level implementation plan to meet its legislative responsibilities under PL 110-53; TSA will enhance the functionality of the pilot program prototype.

2.6 EPA wants to implement a hazardous waste electronic manifest program.

EPA wants to use a business approach in which a private company would build and operate a national hazardous waste e-manifest processing center.

EPA is interested in promoting e-manifest use and is considering a model in which a private company would build and operate a national processing system for hazardous waste electronic manifests. The system would be connected as a node to EPA's Centralized Data Exchange (CDX), and data would flow into CDX as e-manifest transactions take place. EPA would allow the company to collect fees in exchange for building and operating the national e-manifest system.

This section describes EPA's initiative to develop its electronic manifest regulatory program and EPA's difficult experience in attempting to implement a national e-manifest processing center. **Figure 2.6.a** illustrates how EPA's e-manifest initiative has unfolded over the years. The following sections describe EPA's experience in more detail.

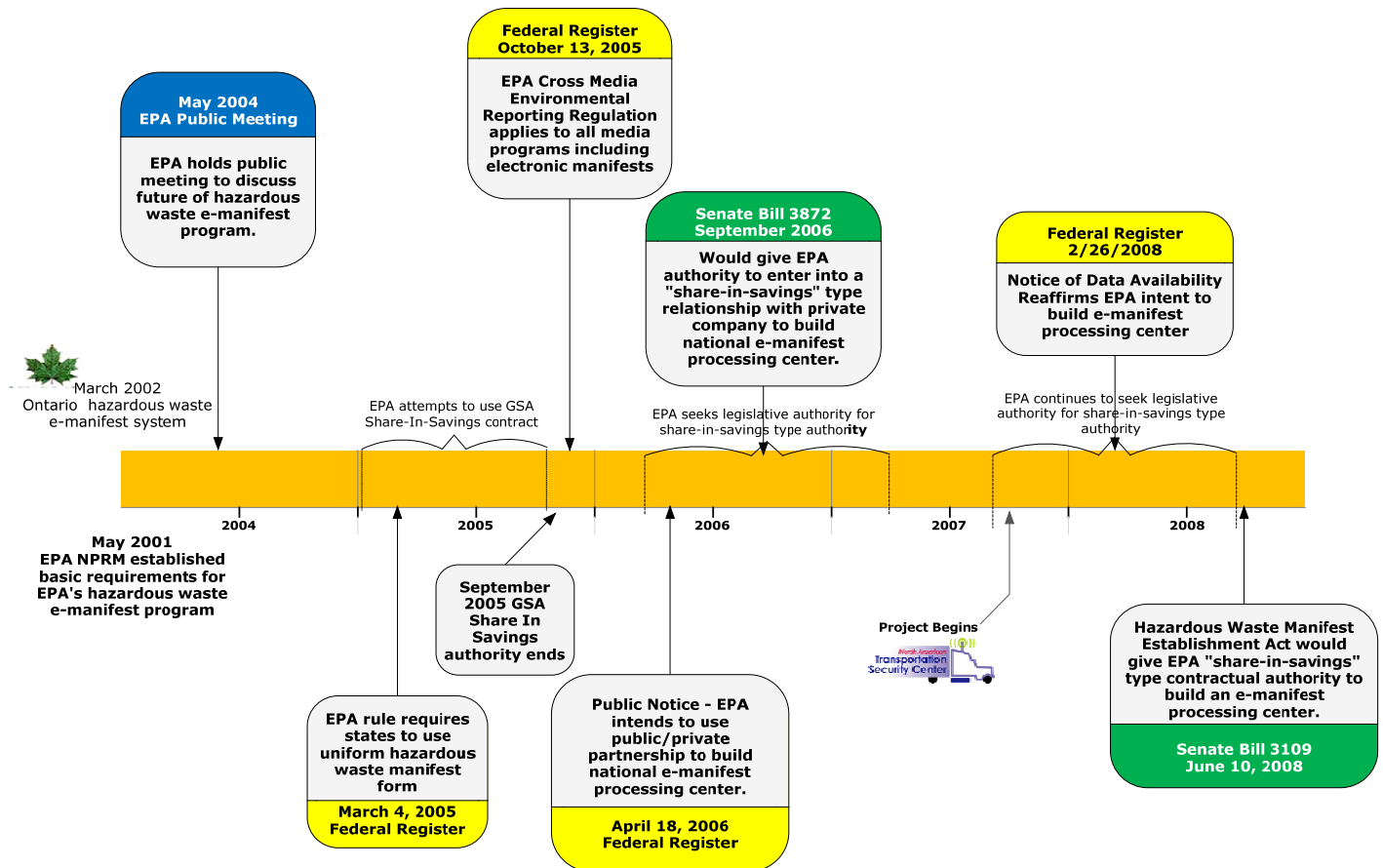


The hazardous waste manifest system has been in place in the U.S. since 1980.

2.6.1 EPA's hazardous waste manifest requirements are burdensome and expensive.

Since 1980, the hazardous waste manifest system has provided a paper trail to track hazardous waste shipments from "cradle to grave." Waste generators, transporters, and waste management firms each participate in documenting the movement of waste shipments through the use of the current paper manifest system. The current "as-is" manifest business process is illustrated in **Appendix A**. A copy of the hazardous waste manifest form may also be found in **Appendix A**.

Figure 2.6.a Timeline for EPA's electronic manifest initiative.



About 28 states currently collect completed manifest copies from hazardous waste generators and waste management facilities, manually keying or scanning the data into state tracking databases. These states utilize manifest data for program management, for identifying trends in waste management, for enforcement and for assessing waste management fees.

EPA estimates that there are there are 2.2-5 million hazardous waste shipments in the United States each year. Given the volume of manifests circulated each year and the number of copies that must be signed sequentially and retained in files for inspection, the paperwork burden attributed to the manifest system is one of EPA's largest. EPA estimates that the paperwork burden associated with its hazardous waste manifest is about 3 million person-hours per year and costs waste handlers and states between \$193 million and \$595 million per year.

EPA's expects e-manifests will reduce paperwork burden on industry and government agencies.

2.6.2 Electronic manifests have the potential of generating savings of more than \$300 million/year.

Electronic manifests will save money. On a unit cost basis, EPA estimates that an e-manifest transaction will generate cost savings of about \$75/manifest. As illustrated in **Figure 2.4.b** cost savings will be captured by waste generators, waste transporters, waste firms, and state agencies. With about 4 million hazardous waste shipments in the U.S. each year, electronic manifests have the potential to generate savings of more than \$300 million per year.^{19 20}

Electronic manifests have the potential of generating savings of more than \$300 million per year in the U.S.

Figure 2.4.b EPA Estimated E-Manifest Cost Savings

	Unit Cost Savings % Distribution	Unit Cost Savings \$ Distribution
Waste Generators	22%	\$16.67
Waste Management Firms	47%	\$34.96
Waste Transporters	20%	\$14.99
State Agencies	11%	\$8.20
EPA	0%	\$0.00
Total	100%	\$74.82

According to EPA, electronic manifests will generate a cost savings of ~\$75 per manifest transaction.

Waste transporters and waste management firms together capture about two-thirds of available e-manifest cost savings – about \$50/manifest transaction. Many waste transporters are captive transporters – ie. they are owned by waste management firms and haul exclusively for their parent companies. When viewed in this light, the waste management firms will be the largest beneficiaries of EPA's e-manifest program. Note that EPA does not capture cost savings under an e-manifest program as responsibility for management of hazardous waste programs is fully delegated to the states. EPA is not a party to the manifest business process and has no operational role in the day-to-day running of the hazardous waste programs in the states.

EPA does not share in e-manifest cost savings because the states run hazardous waste programs in the U.S.

Given the huge paper burden associated with its manifest program, EPA is interested in transforming the manifest system from its current paper-based approach to one that takes greater advantage of electronic information technologies. Successful implementation of an e-manifest system will substantially reduce the costs and paperwork burden associated with the current manifest system, improve the ability to track waste shipments and improve the quality and timeliness of manifest data.

¹⁹ EPA estimates that there are 2.2-5 million hazardous waste manifest transactions in the U.S. each year. The hazardous waste manifest unit cost figures are from the 2002 EPA Hazardous Waste Cost/Benefit Analysis – Table 5-12, *Unit Cost Savings Over As-Is Model*.

²⁰ A later study for EPA by the Logistics Management Institute in 2002 estimated that a centralized e-manifest system tied to EPA's CDX would generate savings of at least \$100 million/year

2.6.3 EPA wants to build a national hazardous waste e-manifest processing center using a public/private partnership.

EPA wants to build a national hazardous waste e-manifest processing center using a public/private partnership.

As illustrated in **Figure 2.6.a**, EPA has labored for a considerable time to introduce electronic manifests. Initially in 2001, EPA planned to issue a rule that would allow companies and states to use e-manifests. EPA expected that the market would respond and that the states and the regulated community would adopt e-manifest programs without a direct EPA implementation role. EPA moved away from that position over time and began to envision a more direct implementation role for itself.

In 2004, EPA tried to use federal “share-in-savings” contracts to enter into an arrangement with a private company that would build and operate a national e-manifest processing center. The private company would build and operate the system at its expense and recover its costs through an e-manifest processing fee. EPA was unable to use the “share-in-savings” approach and in 2006, sought legislation that would provide the agency “share-in-savings” type authority. EPA’s first legislative initiative failed, and in June 2008, a new legislative initiative began.

Sections 2.6.3.1 – 2.6.3.8 describes EPA efforts over time to build a national hazardous waste e-manifest processing center and the current status of EPA’s efforts.

2.6.3.1 EPA’s original electronic manifest NPRM in 2001 established basic e-manifest requirements.

In 2001, EPA published its vision for an electronic manifest program. It addressed technical standards and EPA’s implementation role.

On May 22, 2001, EPA published a notice of proposed rulemaking (NPRM) aimed at reducing the manifest system’s paperwork burden on users, while enhancing the effectiveness of the manifest as a tool to track hazardous waste shipments from the site of generation to treatment, storage, or disposal facilities (TSDFs). The proposed rule included proposed two manifest system reforms: (1) revisions to the manifest form itself and the procedures for using the form; and (2) revisions to the paper-based manifest system aimed at replacing it with a nearly paperless electronic approach for completing, signing, transmitting and storing manifests, and tracking hazardous waste shipments (hereafter, e-manifest).

The proposed e-manifest regulation represented a decentralized approach in which EPA would issue several information technology (IT) standards, and private parties such as waste management firms and IT vendors would develop and market their own e-manifest systems complying with EPA’s standards. The proposed standards addressed such areas as Electronic Data Interchange (EDI) transaction sets and mapping conventions, Extensible Markup Language (XML) representations of the manifest, electronic signature methods, and computer security standards that were viewed as necessary to ensure trustworthy systems and data that would be free from tampering or corruption. Significantly, under the proposed rule approach, EPA’s role would be limited to the development of the e-manifest standards, and the Agency would not have had any role in developing an IT system or in collecting electronic manifests.

The proposal discussed the type of standards that EPA intended to develop. These standards included a minimal set of controls and procedures applicable to computer systems that would prepare and process electronic manifests. EPA expects these system controls, when combined with the requirement that electronic manifest copies be signed with secure types of electronic signatures, would assure users and regulators of the authenticity and integrity of electronic manifest records. Specifically, EPA expected the proposed electronic signature requirements and computer security controls would address five key issues related to the reliability and enforceability of electronic documents.

- **Identity.** The proposed controls would assist in demonstrating who affixed their signature to the document. Specifically, such controls as access checks, audit trails, signature agreements, and/or signature verification processes would help prevent unauthorized use of electronic signatures.
- **Intent.** The proposed security provisions would assist in showing that the signor acted with the required intent to adopt the document being signed or to be bound

by its contents. This would involve a showing that the signor understood the significance of the signature act, so that he or she could not later repudiate their signature as unintended or mistaken. Signature procedures that include warnings about the consequences of affixing a signature, and an opportunity to review and verify the data presented for signature, would help demonstrate intent.

- **Tamper-resistance.** The proposed security provisions would also assist in demonstrating that a document was not altered after signature, since the ability to alter data after signature would permit the signor to later repudiate a document as different from the one that he or she actually signed. Signature methods that use encryption processes to inextricably bind the signature to the data signed would safeguard electronic documents from subsequent alteration, as would system audit checks that would disclose any changes to a record, or attempts to change a record.
- **Availability.** Copies of electronic manifests would be maintained in such a manner as to be accessible throughout the record retention period. System controls which require the retention of information on software and hardware versions used to create archived records, as well as requirements to retain and maintain previous versions of software, hardware, and system documentation, would ensure that this capability is not compromised.
- **Interoperability and error detection.** Systems that would exchange electronic manifests would be interoperable, so that data are accurately and reliably processed, signatures verified, and security features necessary to data integrity maintained throughout the exchange of the electronic documents. In addition, electronic systems would be able to detect errors (i.e., altered/corrupt data or invalid signatures), so that invalid records can be flagged and corrected. System security controls, validation requirements, signature verification requirements, and requirements to respond to detected errors and invalid signatures can minimize the possibility of invalid documents being passed by electronic systems.

In the 2001 NPRM, EPA described its criteria for the electronic manifest program.

Prior to issuing its NPRM, EPA conducted a small pilot program to test basic e-manifest technology. As part of the pilot, EPA used an early electronic forms product and melded it to a workflow software package to build a crude working prototype of an electronic manifest.

The electronic manifest "forms" EPA used in its pilot tests retained both the form structure and the manifest data, and were signed with digitized signatures using a commercial signature software package. The electronic manifest in the pilot tests had the following functionality.

- Retention of all the graphical elements familiar to the paper form. The manifests could be processed (prepared, signed, transmitted, and stored) in an entirely digital manner, or printed in hard copy.
- Inclusion of numerous on-line help features and edit checks, to assist users with the process of completing the manifest accurately and quickly.
- Packaging of form structure and data together in a single file that could be easily archived and retrieved.
- Integration with workflow or work group software so that the manifests could be routed to appropriate trading partners, while complying with organizations' specific business processes and logic rules.
- Support for mapping data directly to a variety of back-end data bases, including Oracle, Sybase, SQL Server, and ODBC-compliant data bases.

EPA acknowledged electronic forms in terms of the value they hold for an electronic manifest system.

Public comments on EPA's proposed rule indicated diverse and substantial levels of support for an e-manifest system, but cast doubt on the viability of EPA's assumption that waste handlers or others would develop and broadly deploy low-cost, interoperable systems. EPA decided to defer final action on the e-manifest portion of the May 2001 proposed rule and to examine alternatives to its proposed approach.

2.6.3.2 EPA held a public meeting in May 2004 to discuss the future of its e-manifest program.

EPA explained in the 2001 proposed rule that it did not collect paper manifests from the public, nor did it intend to create either a centralized reporting system for electronic manifests or a national data base for tracking manifest data. While the Agency desired to foster the development of electronic manifest systems by issuing national standards that would guide the system development efforts of private parties, EPA did not envision playing a role with respect to electronic manifesting that was any different from the standard-setting role the Agency had played in the past with respect to the Uniform Manifest paper form.

However, a number of public comments criticized the decentralized approach and instead stated that the e-manifest system would be unreliable without a nationally centralized approach under which EPA would develop a single national IT system to host e-manifest services. Lobbyists for the commercial waste management industry were particularly critical of EPA's approach and pressed for an EPA centralized approach.

In May 2004 EPA held a two-day public meeting to discuss the future of its e-manifest program. EPA presented as a favored option the idea of a centralized e-manifest processing center, and drew out of its discussions with meeting participants that there was a consensus of opinion that EPA should pursue the centralized option. EPA also presented the idea of using a public/private partnership to build a national e-manifest processing center. In exchange for building and operating the e-manifest system, the private developer would be allowed to collect e-manifest transaction fees.

EPA's interest in a public/private partnership to build the national e-manifest system is, in large part, a reflection of the fact that EPA's lacks sufficient budget capacity to internally fund development of an e-manifest system. Instead, it has to rely on private capital to support development its development.

2.6.3.3 EPA's uniform manifest rule and its Cross Media Environmental Reporting Rule (CROMERR) laid the foundation for an e-manifest rule.

After the May 2004 public meeting, EPA began issuing rules to pave the way for a national hazardous waste e-manifest program.²¹ On March 4, 2005 EPA published a rule in the *Federal Register* that established a uniform national manifest form. Under the old rule, States were allowed to add additional data fields to the standard manifest form. EPA's rule eliminates that option for states. Since September 4, 2006, all jurisdictions use the exact same form. A copy of the uniform hazardous waste manifest form may be found in **Appendix A**.

The March 4th rule also presented a fundamental shift in the relationship between waste generators and waste transporters. The rule discusses the new role of "offeror" in the EPA hazardous waste manifest process. The status of an offeror is well developed under DOT's hazardous materials regulations. Under DOT rules, an offeror is any person involved with performing certain "pre-transportation" functions that occur before hazardous materials are transported in commerce. An offeror may prepare shipping papers on behalf of hazmat shippers and sign the shipper's certification on the DOT shipping papers. EPA has adopted DOT's concept of offeror, and will allow offerors to sign hazardous waste manifests on behalf of the waste generator. The preamble discussion describing EPA's new offeror role may be found in **Appendix A**.

On October 13, 2005 EPA published the **Cross Media Environmental Reporting Rule** (CROMERR 40 CFR Part 3) in the *Federal Register*.²² CROMERR provides a uniform, technology-neutral framework for electronic reporting across all EPA programs; allows EPA programs to offer electronic reporting as they become ready (without any additional rule-making beyond CROMERR); provides states with a streamlined process – together with a uniform set of criteria – for approval of their electronic reporting implementations

In May 2004, EPA reversed its position on its implementation role. EPA would build a centralized system in conjunction with a private partner.

EPA now requires states to use the same hazardous waste manifest form.

EPA will recognize a new character in the manifest business process – the "offeror". An offeror may prepare and sign a manifest for a hazardous waste generator.

²¹ EPA regulation – uniform hazardous waste manifest form <http://www.epa.gov/fedrgstr/EPA-WASTE/2005/March/Day-04/f1966.htm>

²² EPA regulation – Cross Media Environmental Reporting Rule - <http://www.epa.gov/fedrgstr/EPA-GENERAL/2005/October/Day-13/g19601.htm> <http://www.epa.gov/cdx/cromerr/index.html>

for all their EPA-authorized programs; and ensures that electronic reporting under EPA and EPA-authorized state programs does not compromise the enforceability of environmental programs. Specifically, CROMERR's electronic reporting (ER) provisions:

- modified existing requirements in the Code of Federal Regulations (CFR) to remove any obstacles to ER and allow regulated entities to submit any report electronically, but only after EPA announces that ER is available for the specific report;
- required submission of electronic reports to EPA's Central Data Exchange (CDX) or to another designated EPA system;
- required validation of electronic signatures on reports submitted to EPA through CDX (or another designated EPA system) and ensured that valid electronic signatures have the same legal force as their "wet-ink" counterparts; and
- set forth requirements that EPA-authorized programs must satisfy when implementing ER, and provided a streamlined process for these programs to get EPA approval of their ER implementations.

CROMERR is an EPA agency-wide rule that establishes electronic reporting standards for all EPA programs including standards for digital signatures, data integrity, and identity authentication. EPA's future hazardous waste e-manifest rule will incorporate the requirements of CROMERR by reference.

As an Agency-wide rule, CROMERR is important because: 1). it sets the design/operating standards that a hazardous waste e-manifest system must meet; 2). it establishes e-manifest requirements for state authorized programs; and 3). it establishes the foundation for EPA's upcoming hazardous waste e-manifest rule. CROMERR establishes the infrastructure for EPA's hazardous waste e-manifest program. Of particular relevance is Section 3.200 which establishes requirements that state electronic document receiving systems must meet. Relevant text from Section 3.200 may be found in **Appendix A**.

2.6.3.4 EPA's attempt to use GSA's Share-In-Savings contract program in 2005 was unsuccessful.

Based on the mandate EPA believed it captured in its May 2004 public meeting, the Agency began to explore models for building a centralized hazardous waste e-manifest processing center using a public/private development approach. EPA entered into discussions with the **General Services Administration (GSA)**, which managed the E-Gov Act Share-in-Savings program, on a possible procurement action that might have enabled the centralized e-manifest system to be developed and operated for EPA by an information technology (IT) vendor under a "Share-in-Savings" (SiS) type contract.

The SiS IT contracting mechanism was authorized under the E-Gov Act of 2002 on a provisional basis as an innovative tool for Federal agencies to develop new IT systems with little direct Federal investment. The premise of the SiS contracting approach was that the IT vendor awarded an SiS contract would build the IT system at the vendor's initial expense, and then recover its costs and profit from the cost savings or enhanced revenue that results to the sponsoring agency from the new IT system. With this approach, for example, the successful e-manifest IT contractor would have incurred the initial financial risk and outlay to build the centralized e-manifest system to meet EPA's performance objectives, and then would have recovered its costs and earned its agreed profit from the revenue stream generated by the service fees paid by the users for manifest transactions.

In a 2002 study by the Logistics Management Institute, EPA estimated a centralized e-manifest system tied to EPA CDX would have **start-up costs ranging from \$2.0 million to \$7.0 million in the initial year (2002 dollars), plus \$0.8 million to \$3.2 million per year for future annual operation and maintenance (O&M).**

EPA's plan to use the GSA share-in-savings contract program to build a national e-manifest system suffered a major setback in January 2006 when the Federal Acquisition Regulation (FAR) Council, the group that sets federal acquisition rules, withdrew a rule it proposed in 2004 that would have set parameters for share-in-savings contracting. The FAR Council withdrew its proposed rule after Congress chose to not renew statutory authority for share-in-savings contracts that expired in September 2005. The Congressional decision was influenced by a U.S. Government Accounting Office (GAO)

EPA's Cross Media Environmental Reporting Rule defines the systems infrastructure for e-manifest reporting systems.

EPA's e-manifest rule will incorporate EPA's CROMERR requirements by reference.

EPA tried to use GSA's Share-In-Savings contract mechanism to enter into a contract with a private company to build and operate its e-manifest system.

An EPA study estimated that it would cost \$2-\$7 million to build a centralized e-manifest system tied to CDX, and would cost \$0.8-\$3.2 million/year to operate (2002 dollars).

study issued July 2005 that focused on problems with the share-in-savings program and barriers to its acceptance by government agencies.²³

Effectively, EPA was left without a clear path forward for implementing a national hazardous waste e-manifest processing center.

2.6.3.5 EPA's Public Notice (*Federal Register* April 18, 2006) reaffirmed EPA's intent to use a public/private partnership.

In 2006, EPA reaffirmed its intent to build a national e-manifest processing center and published its vision for the system.

On April 18, 2006 EPA issued a *Federal Register* notice stating the Agency's intent to move forward with its e-manifest rule and its interest in building a **national hazardous waste e-manifest processing center**.²⁴ EPA explained that it was considering a model in which a private developer would build and operate the e-manifest system. The system would be connected to EPA's Centralized Data Exchange (CDX) and would be built to meet EPA CROMERR requirements. Data would flow into CDX as e-manifest transactions take place. The private developer running the national processing center would collect e-manifest transaction fees in exchange for incurring the cost of building and operating the national e-manifest system.

EPA's Public Notice set the stage for a push to obtain GSA share-in-savings type authority via legislation.

The following is a direct extract from the April 18th Public Notice that described EPA's vision for a centralized e-manifest system.

The Agency's General Approach to a Centralized E-Manifest System

Today's notice announces that EPA's preferred approach, at this time, for proceeding with the e-manifest rule is to develop a centralized web-based IT system that EPA will host on its IT architecture. This national system likely would be funded, in whole or in part, by service fees that would be paid to EPA or its contractor. This notice discusses a conceptual design of the nationally centralized e-manifest system and requests comment on our approach.

Today, we are announcing that EPA intends to develop a final rule to authorize the use of electronic manifests that are created and transmitted through the use of a centralized e-manifest system. EPA will consider the comments received pursuant to this notice, along with comments on the e-manifest proposal in the May 2001 proposed rule and the May 2004 Stakeholder meeting, as we prepare a final rule on the e-manifest. The final rule would amend existing manifest regulations which require manifests to be created only as paper forms. These regulatory changes would be necessary to ensure that electronic manifests are as valid as the traditional paper manifests that are signed with ink and manually processed and transmitted. The usage of EPA's national e-manifest system to obtain and process valid electronic manifests would be the key component of the final rule. EPA believes that as a result of this change in approach for the e-manifest system, the final regulation authorizing the use of electronic manifests would be much simpler than the regulation suggested by the May 2001 proposed rule.

The final rulemaking will be constrained in its scope to authorizing the use of electronic manifests created and transmitted in the national system, and to several other key policy issues that must be resolved prior to implementation. EPA thus expects to limit, as far as possible, the subject matter of the final rule on electronic manifesting to the key policy issues associated with authorizing the use of electronic manifests and with implementing the electronic manifest as a means of tracking hazardous waste shipments and recording and transmitting waste shipment information. EPA believes it is far more sensible to address the more detailed technical system design and performance requirements for the centralized e-manifest system within the contracting process than to codify performance requirements and other technical matters within the rulemaking process. We also recognize that State participation and input during the planning stage of the e-manifest development process is critical, because there will be significant

²³ July 2005; U.S. Government Accounting Office: *Share-In-Savings Initiative Not Yet Tested* <http://www.gao.gov/new.items/d05736.pdf>

²⁴ EPA Public Notice, *Federal Register*, April 18, 2006. <http://www.epa.gov/fedrgstr/EPA-WASTE/2006/April/Day-18/f5745.htm>

implementation issues associated with moving to an electronic manifest system. EPA will work closely with our State partners as we develop both the final rulemaking and the detailed system design and performance requirements.

Conceptual Design of the E-Manifest System

The centralized e-manifest system will include the necessary applications and components to supply, complete, electronically sign, transmit, and retain electronic manifests. The centralized e-manifest system that will be developed initially will provide only the core services necessary to manage the basic waste shipment tracking and waste data collection functions of the manifest process, including manifest creation, completion, signing, routing and communication services (i.e., services required to create, view, update, transmit, and close manifests) and the collection, distribution, and archiving of official manifest records. In accordance with requests expressed by stakeholders in the May 2004 public meeting, the system initially will not support any more advanced reporting or business integration services. The system would be designed with scalability so that additional EPA reporting functions (e.g., Biennial Report integration or transboundary waste reporting), or additional commercial services that may be desired by users could be added as future upgrades.

The development of the e-manifest system will use a web services-oriented architecture and will be hosted on EPA's CDX (<http://www.epa.gov/cdx>) and NEIEN architecture. The CDX would act as the Agency's central reporting hub for receiving, processing, and routing the in-bound electronic manifests to waste shipment management entities and to state governments. As the e-manifest would be hosted within our CDX/Exchange Network architecture, the submission of e-manifests to the national system would be governed by the standards and procedures included in EPA's Cross Media Electronic Reporting Rule (CROMERR), which EPA published in the Federal Register on October 13, 2005 (70 FR 59847). The CROMERR Rule provides the legal and policy framework for electronic reporting to the CDX hub, and will address such matters as user registration, user authentication, execution of electronic signatures, and the procedures for producing records of electronic manifest submissions.

The e-manifest system will:

1. Use a web services-oriented architecture
2. Be hosted on EPA's CDX and NEIEN architecture
3. Be compliant with CROMERR
4. Use web-services supported by CDX
5. Use XML for the electronic exchange of e-manifest data

We believe that the use of a services-oriented architecture involving web services applications will enable a high level of interoperability with users' legacy and future system investments. Thus, EPA plans to develop the e-manifest applications in conformance with Internet "web services" standards which now are supported by CDX. Also, schemas (i.e., models for describing the structure of information within a document to allow machine validation of document structure) and stylesheets developed in the Extensible Mark-up Language (XML) will be the means EPA will use for the electronic exchange of e-manifest data, and these XML documents will conform to the data elements of the hazardous waste manifest (EPA Form 8700-22) and continuation sheet (EPA Form 8700-22A) that EPA recently announced in the March 4, 2005 Form Revisions final rule (70 FR 10776).

EPA further will develop the e-manifest applications with the appropriate access controls to ensure that only authorized users may enter the system, complete and sign manifests, and access manifest data. We plan to limit access to particular manifest records and related data to only those entities that are involved with the handling of a waste shipment, as well as to RCRA regulators. The centralized e-manifest system also will support, as far as possible, the provision of reliable and uninterrupted manifest services to the user community and will adopt necessary measures and controls that meet EPA and Federal policies for protecting information security, privacy, and confidential business information (CBI).

2.6.3.6 EPA supported an unsuccessful legislative attempt to gain "share-in-savings" type authority (Senate Bill 3871 – September 2006).

With the demise of GSA's share-in-savings program, EPA sought legislative authority to implement a private contracting approach for its e-manifest program. Senate bill S. 3871, the *Hazardous Waste Electronic Manifest Establishment Act*, was introduced by Sen. John Thune (R-SD) in September 2006. It would have given EPA share-in-savings type authority to implement a hazardous waste e-manifest program.

EPA supported Senate Bill 3871 that would have given EPA share-in-savings type authority. The bill was unsuccessful.

Below is a summary of the bill from THOMAS.

Hazardous Waste Electronic Manifest Establishment Act - Amends the Solid Waste Disposal Act to require the Administrator of the Environmental Protection Agency (EPA) to establish a hazardous waste electronic manifest system that may be used by a hazardous waste generator or transporter, an owner or operator of a hazardous waste treatment, storage, recycling, or disposal facility, or any other entity that is required to use a manifest to comply with any federal or state requirement to track the shipment, transportation, and receipt of hazardous waste or other material that is shipped from the generation site to an off-site facility for treatment, storage, disposal, or recycling.

Authorizes the Administrator to: (1) impose service fees on users to pay for developing, operating, maintaining, and upgrading the system; and (2) deposit the fees into the Hazardous Waste Electronic Manifest System Fund (established by this Act).

Requires the Administrator to: (1) establish the Hazardous Waste Electronic Manifest System Governing Board; and (2) carry out this Act in each state unless the state program is fully authorized to do so.

Hearings were held on the bill on September 28, 2006. The bill, however, languished in the aftermath of the November elections and changes in Senate and House committee assignments. It failed to move beyond the Senate Committee on Environment and Public Works.²⁵

2.6.3.7 EPA's Notice of Data Availability (*Federal Register* February 26, 2008) reaffirmed EPA's intent to seek a public/private partnership via e-manifest legislation.²⁶

On February 26, 2008, EPA published a Notice of Data Availability in the *Federal Register*. The notice reaffirmed EPA's intent to issue an electronic manifest rule and to seek federal legislation giving it share-in-savings type authority to support implementation of a national e-manifest processing center. A passage from the notice describes EPA's intent but issues a caution that promulgation of an e-manifest rule is contingent on EPA gaining legislative authority for e-manifest user fees.

"We are currently developing the final rule that will authorize the use of electronic manifests, and will address scope and other policy issues. However, the promulgation of this rule is contingent upon the enactment of legislation providing EPA the authority to collect user-fees to fund the development and operation of the system. Nevertheless, we continue to move forward with the rulemaking in anticipation of enactment of the needed legislation."

The notice also asked for comment on a refinement to EPA's implementation plan for its e-manifest processing center. EPA expects e-manifest use will be voluntary and that many manifest transactions will continue to be paper based. However, EPA recognizes that a manifest database that holds data on only electronic transactions would be less valuable than one that holds both electronic and paper transactions. EPA has proposed for comment a plan to amend its manifest regulations so that the final destination facility (and only the destination facility) would mail a copy of the completed manifest form to the e-manifest system operator. The system operator would scan the form and enter manifest data from it into the national manifest database. EPA expects the final destination facility would pay the cost of data processing for paper manifests.

This proposal will likely have a huge impact on EPA's manifest operations center. E-manifest use would be purely voluntary. Unless companies moved voluntarily to e-manifest use, most of the transactions would be paper-based making document processing the main focus of the national e-manifest processing center. EPA expects the destination facility would mail a final copy of the manifest to the system operator and pay a fee to the system operator for paper manifest processing. In the February 26th notice, EPA estimated that the charge that the system operator might charge TSDFs for

EPA believes its e-manifest program's success is contingent on EPA gaining legislative authority to collect e-manifest user fees.

EPA wants the e-manifest processing center to process paper manifests. The operation may shift heavily to document processing.

Waste management firms would pay paper processing costs. EPA expects the manifest system operator could scan and enter data from a paper manifest for \$.25 to \$.75/manifest. The waste management trade association has doubts about EPA's cost estimate.

²⁵ For background refer to "BIPARTISAN E-MANIFEST WASTE BILL FACES TIME CRUNCH IN SEEKING PASSAGE" http://www.acetransition.net/images/EPA_Release.doc

²⁶EPA Notice of Data Availability, *Federal Register*, <http://edocket.access.gpo.gov/2008/E8-3615.htm>

receiving paper manifests and for transferring (i.e., imaging and keypunching) paper manifest data to the e-Manifest system, could be between \$0.25 to \$0.75 per paper manifest. TSDFs would incur additional paperwork burden costs for submitting a copy of the final manifest bringing the TSDFs total cost to about \$3.20/manifest.

In its comments, the Environmental Technology Council – the trade association representing the commercial waste management industry (TSDFs) - questioned EPA's cost estimate that it would cost \$3.20 per manifest to convert the manifests to electronic format.²⁷

"If the fee per paper manifest is actually in the neighborhood ... of \$3.20 per conversion, we think that would be acceptable," the council said. However, it noted, EPA has estimated that converting a paper-submitted Toxics Release Inventory Form R would cost \$50 each, meaning the estimate for manifests could be much lower than the real cost.

"If the cost of processing paper manifests approaches this amount, then the [Feb. 26 NODA] does not adequately lay out the real options for comment," the council said. The council also suggested the fee system could be phased in to serve as an incentive for facilities to switch to the e-manifest system.

"If the e-manifest system is well designed and operated, then the number of paper manifests that need to be converted will decrease steadily over time," ETC said.

EPA's preamble discussion on EPA's proposed changes to the e-manifest process may be found in **Appendix A**.

2.6.3.8 Senate Bill 3109, Hazardous Waste Manifest Establishment Act, was introduced by Senator John Thune (R-SD) on June 10, 2008

Senator John Thune (R-SD) introduced Senate Bill 3109, the Hazardous Waste Establishment Act, on June 10, 2008. Co-sponsors of the bill are Benjamin Cardin (D-MD), Amy Klobuchar (D-MN), and Frank Lautenberg (D-NJ). S.B. 3109 is, in essence, a repeat of Senate Bill 3871 that was introduced by Senator Thune in September 2006 (refer to Section 2.6.3.6).

Senate Bill 3109 will amend the Solid Waste Disposal Act (42 U.S.C. 6921) and will require the EPA Administrator to establish a hazardous waste electronic manifest system within three years. S.B. 3109 will give EPA "share-in-savings" type contract authority. EPA will be authorized to issue a contract to a private party that would build and operate the electronic manifest system. The party would be allowed to collect a manifest processing fee to recoup its investment costs and generate a profit. On July 31, 2008 the Senate Committee on Environment and Public Works ordered Senate Bill 3109 to be reported without amendment favorably.

2.7 The Alliance for Uniform Hazmat Transportation Procedures was established by state agencies to preserve state prerogatives in hazmat permitting and registration.

The Alliance for Uniform Hazmat Transportation Procedures (the Alliance) is a

state-based organization that operates in conjunction with the **National Conference of State Legislatures** (NCSL).²⁸ The Alliance was established in 1990, and supports state registration and permitting programs for motor carriers that transport hazardous materials and hazardous waste.

The Alliance was established under Section 22 of the Hazardous Materials Transportation Uniform Safety Act of 1990 (HMTUSA). Section 22 mandates that states that elect to

E-manifest transaction volume would grow slowly if the waste management industry sets the implementation parameters for an e-manifest program.

Senate Bill 3109 will give EPA the authority to contract with a private company to build and operate a national hazardous waste electronic manifest system.



The Alliance for Uniform Hazmat Transportation Procedures is sponsored by the National Conference of State Legislatures, and has a Congressional mandate to support state hazmat programs.

²⁷ Hazardous Waste - Industry Questions Suggested Changes to E-Manifest Proposal, BNA Bulletin May, 5, 2008 <http://subscript.bna.com/SAMPLES/ecb.nsf/85256269004a991e8525611300214487/0311855b6e883f418525743b0071d3a8?OpenDocument>

²⁸<http://www.hazmatalliance.org/>
<http://www.ncsl.org/programs/transportation/ALLHAZMAT.htm>

register and permit motor carriers that transport hazardous materials must do so using uniform application forms and uniform procedures.

2.7.1 Why was the Alliance established?

In 1990, the states were faced with the prospect that their permitting and registration programs for carriers of hazardous materials would be wiped out - preempted by a potentially weaker federal law. At the urging of the trucking industry, Congress was on the verge of doing away with state programs and replacing them with a one-size-fits-all federal program.

State negotiators led by the NCSL and the **National Governors Association** agreed to convene a working group of state officials that would craft a model program for hazardous materials transportation permits and registration using the best practices of existing state programs. However, part of the deal was that the new state-developed "Uniform Program" would preempt existing state programs. In essence, the states agreed to preemption of individual state programs, albeit on state terms, to save an existing and important area of state regulation.

States have the option of joining the Alliance and adopting the Alliance's uniform program. Otherwise, they are subject to federal hazmat registration and permitting programs administered by the FMCSA. Under the terms of Section 22, FMCSA will implement the Alliance Uniform Program once 26 states have adopted it. The Alliance has the full support of the FMCSA and is currently funding the centralized aspects of the Uniform Program. Informally, the FMCSA has indicated a willingness to lower the target implementation threshold to 18-20 states from the current 26 state target.

The Alliance currently consists of seven member states - Illinois, Michigan, Minnesota, Oklahoma, Nevada, Ohio, and West Virginia - that have implemented the Uniform Program. Other states, such as Alaska and Missouri, are in the process of joining the Alliance. States have the option of implementing part or all of the Alliance's Uniform Program. As illustrated in **Figure 2.7.a**, states may choose to register and permit all hazmat shipments (including hazardous waste and radioactive materials) or hazardous waste shipments only.²⁹

2.7.2 What is the Uniform Program?³⁰

Protection of public health and safety is the main objective of the Uniform Program. The two main mechanisms of the Uniform Program are: 1). carrier registration; and 2). carrier permitting.

Registration provisions of the Uniform Program are designed to:

- identify persons who transport, ship or cause to be shipped hazardous materials by motor carriers, and
- generate revenues for state hazmat programs.

Permitting provisions of the Uniform Program's permitting are designed to:

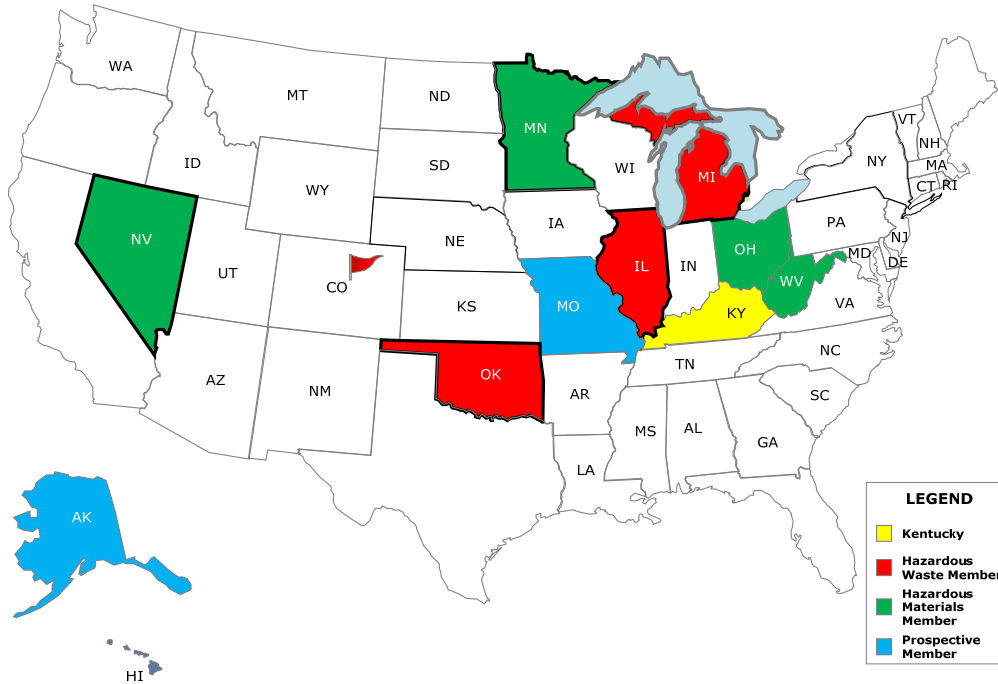
- identify "qualified" motor carriers of hazardous materials; and
- ensure states participating in the reciprocal agreement that the base state is operating in accordance with Alliance policies and procedures.

The Alliance was established to preserve state hazmat programs. Seven states – including three bordering Kentucky – are Alliance members.

²⁹ Hazardous waste is a subset of the much larger universe of hazardous materials.

³⁰ NCSL's website has a on-line overview of the Alliance Uniform Program.
http://www.ncsl.org/slides/transportation/0605hazmat_jpg_files/frame.htm

Figure 2.7.a The Alliance for Uniform Hazmat Transportation Procedures



"The primary goal is to promote a higher degree of public health and safety through uniformity and consistency. The best aspect has been the education of the carriers in our state on safety regulations, insurance and other compliance aspects."

Loretta Bittner, West Virginia Alliance Governing Board

2.7.2.1 The Uniform Program revolves around the "base state" concept.

The Alliance program revolves around the "base" state concept. Instead of registering in multiple states, applying for multiple permits, and paying fees to multiple states, carriers transact all of their business with the state where they travel the most miles. This is the carrier's **base state** and it, in effect, become a "one-stop shop" for the carrier, reducing the carrier's administrative overhead and removing duplicative activities across states.

When a carrier registers in its base state, it gains status as a carrier in all the Alliance states. In addition, permits issued by a carrier's base state are recognized by all Alliance states.

Under the Alliance Uniform Program, base states have the following responsibilities:

- Process the permitting application for each carrier for which it serves as the base state.
- Collect the permit fee associated with the cost to the state of issuing the permit.
- Conduct any pre-permit investigation or audit.
- Issue indicia to the company that must be carried inside each vehicle transporting hazardous materials.
- Determine whether violations of the permitting requirements should result in suspension or revocation of the national permit.
- Perform periodic reviews of the motor carrier's operations.

2.7.2.2 Under the Uniform Program, hazmat carriers must have acceptable safety and operating records.

Under the Uniform Program, Alliance states exercise authority on one another's behalf. Prior to the formation of the Alliance, each state registered and permitted each carrier transporting within its borders. Each state had the final say on who was allowed to transport hazardous materials in the state and on the fees that would be levied on carriers traveling through the state. Under the Alliance base state reciprocity agreement,

Under the Alliance program, hazmat carriers register only with a "base" state. Permits issued by a base state are recognized by all Alliance states.

"Since May '93, a group of states, the Alliance for Uniform Hazmat Transportation Procedures, has been using a common sense approach to hazardous materials registration and permitting, called the Uniform Program. This approach is to foster uniformity of hazardous materials transportation permitting and registration through a single (base) state process. This project is fully supported by the Federal Motor Carrier Safety Administration."

Julie Anna Cirillo, FMCSA

the registration and permitting is handled by the base state and when the base state makes a permitting decision that decision is made on behalf of all Alliance states

Hazmat carriers are required to submit an application to its base state for permission to haul hazardous materials. The base state conducts a review of the motor carrier's qualifications to transport hazardous materials and, if appropriate, issues a permit. Alliance states have agreed to use common criteria to support denial of a permit application by a hazmat carrier.³¹ Some of those criteria include the following.

- Violations of hazmat regulations that pose imminent hazard to the public or the environment.
- Exhibition of reckless disregard for the public or environment.
- False statements in an application.
- An "unsatisfactory" safety rating.³²
- Failure to maintain a satisfactory security plan.
- Failure to comply with regulations in a manner showing motor carrier is not fit to transport hazmat.
- Failure to comply with an out of state order.
- Failure to comply with any other order in a manner showing the carrier is not fit to transport hazardous materials.
- Failure to maintain minimum insurance.
- Failure to maintain RSPA registration.
- Loss of operating rights or suspended registration for failure to pay.

2.7.2.3 Hazmat fees are allocated using the double apportionment method.

The Uniform Program does not mandate a fee structure. States can assess fees as they see fit as long as the revenue is used for hazardous materials transportation activities and do not interfere with interstate commerce. Fees must also meet the fairness test under the dormant commerce clause found in *Evansville* (92 S. Ct. 1349) (1972). This test says a fee is fair if it is based on a fair approximation of use of the state facilities, is not excessive in relation to benefits conferred, and does not discriminate against interstate commerce. "Flat tax" fees assessed per vehicle or per trip per vehicle have been preempted because they fail the "internal consistency" test of the commerce clause as an undue burden on interstate commerce. Essentially, these fees are not equitable to nationwide carriers.

Many hazmat carriers operate in more than one state and have fee obligations to more than one jurisdiction. Under the Alliance program, hazmat carriers register only in their base state and the base state is responsible for collecting appropriate fees and allocating them to other states. This provides convenient "one-stop shopping" for carriers that operate in multiple states, but it also gives the base state the responsibility of collecting revenue for other states, similar to the "double apportionment" fee collection and allocation methodology underlying the International Fuel Tax Agreement (IFTA) and the International Registration Plan (IRP).

The Alliance's "double apportionment" method for fee allocation is based on "hazmat mileage" in a state. For example, assume a carrier's hazmat trucks travels 10,000 miles in West Virginia and 40,000 miles in Ohio. The carrier pays \$25,000 in hazmat fees to Ohio, the carrier's base state. Ohio will collect \$25,000 from the carrier but allocate \$5,000 ($10,000/50,000 * \$25,000$) to West Virginia to reflect the relative percentage of the carrier's hazmat miles traveled over West Virginia's roads.

2.7.2.4 What data do Alliance states collect from carriers?

Figure 2.7.b lists the data that Alliance states collect from carriers during registration and permitting

³¹ Detailed procedures for registration and permitting of hazmat carriers may be found in the Alliance's *Administrator's Manual for the Uniform State Hazardous Materials Transportation Motor Carrier Registration and Permit Program*.

³² The FMCSA provides carrier safety information through the FMCSA's Safety and Fitness Electronic Records (SAFER) System.

Hazmat fees are collected by the base state and allocated to other Alliance states using a double apportionment method.

Figure 2.7.b Data Collected from Carriers by Alliance States.

Part I Registration Application	
Applicant name Employer ID number DBA name if applicable Mailing Address for purposes of correspondence Street Address, if different from mailing address Does address reflect a change in the last 12 months? Person to contact concerning the application Contact title Contact phone number Contact fax number USDOT motor carrier census number Motor Carrier Docket number For intrastate carriers, State ID Number, if applicable USDOT, motor carrier docket #, State ID number(s) displayed on vehicles USDOT HazMat Registration number Federal EPA transporter identification number, if applicable Uniform manifest required?	Alliance member states where transportation of hazardous waste is expected States where hazardous was transported in previous 12 months Transportation of radioactive waste in Nevada Phone number at which the carrier can be contacted Information provided in application covers which 12 month period? Fleet information for carriers with multiple fleets Average number of power units owned, operated, leased, etc. IRP allocation percentages by state and other North American jurisdictions Percentage of total activity that involves hazardous materials IRP account number Average number of cargo tanks owned, operated, or leased with capacities greater/less than 3,500 water gallons Classes, divisions and zones of hazardous materials transported Amount of fee(s) enclosed
Part II – Corporate Structure and Corporate Certifications	
Corporate Structure Type of Carriage Type of Business Number of years the applicant has transported general freight Number of years the applicant has transported hazmat Number of years the applicant has transported hazardous waste Permits Withdrawn, Denied, Suspended, or Revoked USDOT Safety Rating Most recent USDOT Safety Rating History of applicants major violations related to hazmat Assessed or paid fines over \$1000 Fined or convicted in last 3 years of transporting hazmat without permit Has subsidiary, etc. been found culpable in legal proceedings Reportable Hazardous Materials Transportation Incidents - Incidents required to be reported under 49 CFR 171.15 (a) (1)	Terminals - Number and address of all terminals owned or operated Inspections - Certification that vehicles have undergone required periodic certification Financial Responsibility Certification that the applicant executed Form MCS82 or MCS90 Location of the form Insurance Information Other Certifications Current commercial drivers licenses Complies with USDOT bulk packaging Emergency Response Plan State designated routing requirements Training requirements for hazardous materials employees Retention of shipping papers Hours of Service Applicant meets motor carrier safety requirements Meets federal security requirements for shipments of hazardous materials
Part III Additional Information Required from Motor Carriers of Hazardous Waste	Part IV General Application Certifications
Incorporation Facilities Owned and Operated Identification of Key Management Personnel Permits Held Related Business Concerns Legal Proceedings	Acknowledging that Applicant is Subject to Audit Certification of Accuracy and Completeness Renewal of Current Registration Certification of no Key Changes, Listing of Certain Key Changes

2.7.3 What requirements does a state have to meet to join the Alliance?

In order to participate states are required to complete the following steps.

1. Complete letter of intent to governing board. A state must inform the Alliance governing board that it requests permission to join both the uniform program and base state agreement. Prior to acceptance into the Alliance, the state will be required to become an official signatory to the base state agreement.
2. Pass enabling legislation. Legislation is required for states to enter into the Alliance and adopt the policies and procedures of the alliance. The enabling legislation can be designed at the state level, but model legislation is available from the Alliance. In order to begin the process the legislation may not have to be finalized. Planning to enact the legislation contingent upon joining the Alliance is sufficient.
3. Designate lead agency. Some states grant jurisdiction for the regulation of hazmat and hazardous waste to separate administrative entities. For this reason, the governor is required to designate a lead agency which will be responsible for compliance. This eliminates the need for other states to keep in contact with multiple agencies within a given state.
4. Request an accreditation review by the board. The accreditation review verifies that a state meets all the requirements for joining the alliance. The review itself is a three step process. First, the board sets standards for each jurisdiction. Second, using those standards each jurisdiction develops an implementation and operating plan. Third, jurisdictions are reviewed, according to board standards and the jurisdictional plan, at application and every three years after that.

The specific standard used by the board may vary by jurisdiction, but they serve to require general criteria. They require that each state have: 1). adequate personnel to implement the uniform program, 2). ability to store essential information and issue credentials in a timely manner, 3). the ability to disseminate essential information to motor carriers, 4). adequate training for personnel, and 5). capacity for the accounting required under the reciprocal system. In addition to these capacity/ability issues, each state must be able to do the following.

- Develop an operating budget and establish an equitable registration fee and a permit application review fee structure.
- Develop a plan to ensure full public participation as outlined in the Uniform Program.
- Ensure motor carrier data confidentiality.
- Provide evidence of sufficient audit capacity to fulfill the audit requirements of the Uniform Program including personnel time and training.
- Demonstrate that all appropriate enforcement officials recognize the Uniform Program credential, regardless of the state of issuance, as adequate for the transport of hazardous materials within the jurisdiction.
- Have any necessary enabling legislation and implementing regulations in place when it enters the Uniform Program agreement.
- Certify that it will operate the Uniform Program pursuant to the policies and procedures developed by the Board.

2.7.4 What oversight does the Alliance exercise over member programs?

As a condition of membership in the agreement, all states must agree to participate in a peer accreditation review team after their first year of operation in the Uniform Program. During a peer review, an accreditation team will examine the following aspects of the state's program.

- *Personnel.* The accreditation team will ensure that the program has adequate staff dedicated to reviewing applications and conducting any necessary background investigations for Part II or Part III permits. The jurisdiction may contract any portion of the work out to other state offices or private contractors. Any agreement that the program has to contract out any portion of the work will also be reviewed. The team will ensure that the program has adequate personnel to receive, process, and disperse funds to other states on a quarterly basis.

States have to meet a number of requirements to gain and retain Alliance membership.

Alliance states must participate in a peer accreditation review program.

- *Automated Data Processing (ADP).* The accreditation team will evaluate the technical resources that are available to conduct the Uniform Program. The state must have the capability to transmit data to a central database and conduct searches of the repositories database including computer resources with adequate internet capabilities. The state must be able to store elements of the registration electronically and issue credentials to carriers in a timely manner.
- *Preparation for Carriers.* The accreditation team will assess the state's marketing and outreach efforts to all covered motor carriers based in the state. The affected industry should have prior knowledge of the Uniform Program implementation date in their base state. The Board recommends that the state conduct at least one full briefing on the Uniform Program for the industry that is co-sponsored by the state trucking association. The state should have a general idea of the number of carriers that will be involved in the program. The new state can also survey their carrier population through the state trucking associations to get an idea of the number of carriers hauling hazardous materials that are based in the state.
- *Training.* The review team will look at training programs and guidance available to all staff members involved in the Uniform Program. Training should result in a general understanding of the Uniform Program and a thorough understanding of the employees' responsibilities under the program, especially those related to reciprocity among the participating states. It is anticipated that the repository will develop training modules for program managers and other program staff covering all aspects of the Uniform Program. Participation in Alliance sponsored training will be viewed as satisfying this requirement. Agency staff should also have a general knowledge of all federal regulations—including employee training regulations—that are referenced in the Uniform Program application.
- *Program Funding.* The review team will ensure that the registration fee is consistent with Uniform Program requirements and will provide the program with sufficient funds to support the registration and permit program in the state. The financial accounting aspects of the state's program will be reviewed to ensure compatibility with program guidelines. The program must have full capability (personnel, computer capacity, etc.) to receive, process and disperse funds to member states.
- *Public Access to Records.* The state must be equipped to register complaints from the public and transmit them to the repository. The public shall have access to information in the repository database and the state office in accordance with all federal and other state freedom of information laws. Information on the nature and evidence surrounding complaints shall be available to the public.
- *Audit Capacity.* Under the base state agreement, the registering state must be able to "conduct audits of motor carriers as necessary to ensure that the carrier is accurately reporting its hazardous materials transportation activity." A state that also issues motor carrier permits also must "perform periodic review of the motor carrier's operations; and conduct investigations or audits of the permit applicants." The accreditation team will assess the program's administrative capacity to audit carriers under the Uniform Program. This will overlap into training criteria, personnel criteria and enforcement capacity.
- *Enforcement.* The state must communicate with appropriate state enforcement officials to identify carriers that are not properly registered and/or permitted under the base state agreement. In addition, the state is responsible for conducting any necessary training of enforcement personnel as to the nature of the base state system and credentials that properly registered/permitted carriers will keep in their vehicles. Each state shall enforce the requirements of the Uniform Program but will maintain fines and penalties established by the law of the participating state.
- *Enabling Legislation and Implementing Regulations.* The state will have enabling legislation and implementing regulations in place before the state may participate in the Uniform Program. During the accreditation review and subsequent reviews, the review team should be aware of any changes that have been made to the Uniform Program and possible changes that may be required to state statutes or agency regulations.
- *Funding Mechanisms in Place.* The state shall enact a fee program consistent with Alliance guidelines.

2.7.5 What are the benefits of state membership in the Alliance? Why is membership lagging?

Alliance membership brings a number of benefits to states.

- *The Uniform Program is well designed, comprehensive, and has stood the test of time.* The Alliance has developed detailed procedures to support state implementation of the Uniform Program. The Alliance procedures have been developed and refined by almost two decades of state experience. The procedures have a proven track record work in minimizing administrative burdens of the states in implementing their base programs.
- *Membership in the Alliance makes it easier for states to implement and defend fee*

"There is not a governor or state legislator who is not looking for ways to make state government more effective and more efficient. The Uniform Program benefits the states by distributing the burden of regulating the nation's interstate carriers among the states. This allows the base state to conduct a more thorough review of the operations of a carrier for which it has responsibility, rather than conducting a less stringent review of every carrier that enters its jurisdiction."

Nancy Brown
State of Kansas
Alliance Governing Board

programs to fund internal programmatic activities. States need revenue to run their programs, and the Alliance program is structured to allow states to capture fees from hazmat carriers in a defensible, reasonable manner. Participation in the Alliance program also helps state administrators justify the collection of hazmat fees.

- *Carrier compliance is enhanced and highway safety/security is improved.* The Alliance reports that carrier compliance with hazmat safety rules is markedly improved by implementation of the Alliance program. The roads are safer and more secure.
- *Less workload and efficient business processes save states money.* Alliance membership helps states share the workload. Instead of registering and reviewing every hazmat carrier in their state, states only register and review those carriers that identify a given state as their base state. This allows each state to focus their attention and resources on a smaller group of carriers without losing confidence that other carriers are also being thoroughly checked. Base states are able to improve the thoroughness of carrier reviews and inspection and capture cost savings from the decreased volume of registration and reviews required.
- *Lower regulatory load for interstate hazmat carriers.* Interstate carriers benefit from the Alliance program. Instead of having a regulatory interaction with many states, carriers interact with only their base state for permitting and registration. A lighter regulatory load saves carriers money.

In June 2008, the Alliance issued a contract to better articulate and quantify the benefits of Alliance membership. The work is not yet complete but was undertaken in recognition that state membership in the Alliance has remained stubbornly low. Informally, Alliance board members have identified issues that they believe are inhibiting state membership in the Alliance.

- It's easier for states to "go-along" rather than to work to "get-ahead". Joining the Alliance takes work and political will to overcome the inertia of the status quo. States have to adopt legislation which takes political will on the part of state program administrators. While Alliance programs usually enjoy strong support from interstate carriers, intrastate carriers are often resistant (and vocal) in their opposition to a hazmat fee program. To date, the benefits versus the "political pain" have not been well articulated by the Alliance.
- The Alliance has not found a mechanism or issue to rally the states to join the Alliance, even though there are significant benefits for state membership. The Alliance has not been able to find and exploit a mobilizing catalyst for state membership.

States have to overcome programmatic inertia to join the Alliance. The benefits are positive, but have not been well articulated by the Alliance. There is not a mobilizing catalyst to drive state membership.

2.8 How will these regulatory/legislative drivers influence the design and operation of the Transportation Security Center?

Figure 2.8.a, summarizes how regulatory/legislative drivers will influence the design and operation of the Transportation Security Center. The yellow-coded portions of the table are focused on hazmat truck tracking. Gold-coded sections focus on hazardous waste electronic manifests and green-coded sections are relevant to both hazmat and hazardous waste.

Figure 2.8.a Implications of regulatory/legislative drivers on the design and operation of the Transportation Security Center

RSPA HM-232 (DOT) – March 25, 2003	
2.2.1	<p>Note: HM-232 was supplanted by TSA guidance (June 2008 – see Section 2.4) but the voluntary guidance issued by RSPA under HM-232 was largely adopted by TSA and is still relevant to hazmat shippers/carriers.</p> <p>Starting with HM-232 in 2003, the hazmat carrier industry has been subject to hazmat security oversight. A model regulatory program embracing the current voluntary procedures in place since 2002 will be familiar to industry, especially carriers of high-risk hazardous materials.</p> <p>RSPA urges shippers (under HM-232) to set up a communications system with transport vehicles and operators, including a crisis communication system with primary and back-up means of communication</p>

among the shipper, carrier, and law enforcement and emergency response officials. The TSC should serve as the vehicle to meet the communications needs of the parties under HM-232.

Shippers and carriers must prepare en route security plans under HM-232. It asks carriers to develop preferred and alternate routing for hazmat shipments. Assume that the model program requires submission of electronic route plans to the Transportation Security Center. The system must be able to accept route plans electronically. The system should also be able to accept multiple route plans from a shipper/carrier (preferred and alternate routes) and a mechanism for the shipper/carrier to select a route when the carrier accepts shipment custody.

HM-232 applies to hazmat shippers as well as hazmat carriers. The universe of hazmat shippers is much larger than the universe of hazmat carriers. Given the numbers, hazmat shippers represent an attractive service target for the TSC, and the needs of hazmat shippers (subject to HM-232) should be fully served by TSC service offerings.

Hazmat Commercial Drivers' Licenses (Patriot Act Background Checks) – January 2005

2.2.2 Since 2005, TSA rules require states to conduct security background checks on drivers before they are issued state CDLs to haul hazardous materials. From a regulatory/systems perspective, TSC systems should prevent drivers without a hazmat extension to their CDLs from picking up a hazmat load.

Shippers should be required to verify that a hazmat carrier has a hazmat CDL and is authorized to accept a hazmat shipment.

Shippers should be prohibited from using a driver without a Hazmat CDL.

A carrier should be prohibited from allowing a driver without proper CDL hazmat certifications to accept a hazmat shipment.

Drivers will need to be linked with companies to prove that an individual driver is authorized to carry goods for a permitted entity. This probably means driver information needs to be collected via company registration. Also, system users need to have the means to edit driver data 24/7 as driver lists may change frequently.

An electronic manifest solution could reinforce checks on a drivers hazmat CDL status. The system could prevent a carrier from assigning a driver without proper credentials. Also, the system could prevent a driver without proper credentials from picking up a hazmat shipment by rejecting the driver's digital signature (assumes the hazmat e-manifest will require digital signatures).

An alert /message needs to be made in the event an unauthorized driver attempts to pick up a hazmat shipment (e.g. no hazmat CDL). An xml message needs to be crafted for this situation and a response workflow needs to be established.

FMCSA Hazmat Safety Permits – January 2005

2.2.3 Note: The list of materials requiring FMCSA hazmat safety permits overlaps with the list of Tier 1 Highway Security Sensitive Materials (HSSMs) published by TSA June 2008 (see Section 2.4). In general, Tier 1 HSSMs will require FMCSA hazmat safety permits.

Under the FMCSA hazmat safety permit program, carriers have to have a communications system that allows the carrier to stay in contact with its drivers. The requirements stop short of en route shipment tracking but TSA's program is clearly heading toward requiring shipment tracking for some hazmat shipments. The model program should initially require tracking of security sensitive hazmat shipments that are subject to FMCSA safety permits.

From a regulatory/systems perspective, TSC systems should prevent carriers without a FMCSA hazmat safety permit from dispatching drivers to pick up materials listed under Section 385.403.

Shippers should be required to verify that a hazmat carrier has a FMCSA hazmat safety permit.

Shippers should be prohibited from using a hazmat carrier without a FMCSA hazmat safety permit.

A carrier without a FMCSA hazmat safety permit should be prohibited from allowing a driver to accept a material listed under Section 385.403.

According to FMCSA, maintaining communications records represents almost the total cost of compliance with hazmat safety permit requirements. FMCSA has explicitly recognized the role that fleet tracking systems may play in helping carriers meet their communications records requirements. TSC systems should be designed to help carriers meet the communications requirements of Section

	<p>385.403.</p> <p>According to the FMCSA, there are about 3,100 hazmat carriers subject to the FMCSA hazmat safety permit requirements. About two-thirds are interstate carriers.</p>
<p>DHS Chemical Facility Anti-Terrorism Standards (CFATS) – April 9, 2007</p>	
<p>2.2.4</p>	<p>The industry voluntary program for chemical plant safety did not work, and DHS was forced to issue its CFATS regulations to require chemical facilities to institute hazmat security programs. This reinforces the idea that regulations need to drive “smart truck” technology deployment and data reporting.</p> <p>The DHS CFATS regulated community largely overlaps with the regulated community (hazmat shippers) under HM-232. But this group will have special hazmat interests in addition to off-site shipment. Like the HM-232 companies, CFATS companies represent an attractive service target for the TSC, and the needs of CFATS customers should be addressed by TSC service offerings.</p>
<p>TSA Highway Security Sensitive Materials Guidance – June 26, 2008</p>	
<p>2.4</p>	<p>TSA described two tiers of Highway Security-Sensitive Materials (HSSM) in its June 2008 guidance. TSA defined Tier 1, the riskiest HSSMs, as HSSMs 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. TSA published Security Action Items (SAIs) for Tier 1 HSSMs. While the SAIs are not mandatory, they clearly define establish the structure for future regulatory programs. Therefore, the model regulatory program should focus on Tier 1 HSSMs and the TSA SAIs associated with Tier 1 HSSM shipments, especially SAI 17 – SAI 23.</p> <ul style="list-style-type: none"> o Shipment routing chosen should result in least public exposure and minimal delay in transit. o The shipper, carrier and receiver must agree on the shipment’s estimated time of arrival (ETA) before the shipment is made. o During transit, carriers should provide updated ETAs to receivers. o Receivers should provide shippers notice if a shipment is late or if the full shipment has not been delivered. o Carriers should establish primary and alternate routes. Routes should minimize proximity to highly populated urban areas or critical infrastructure (bridges, dams, tunnels). o Alternate routes should steer Tier 1 HSSM shipments away from highly populated urban areas or critical infrastructure during Orange or Red alerts. o Drivers should notify carrier dispatch center when deviating from planned route. o Except in an emergency, carriers should maintain expected shipment chain of custody. A load should not be shifted to a different truck nor should driver crews be changed. o Trucks should have in-cab devices that prevent unauthorized drivers from starting the tractor. o Drivers should have access to a panic button – in-cab and/or remote – that sends an alert to the driver’s dispatch center. <p>SAI 23 of TSA’s HSSM guidance is particularly important from a model regulatory perspective.</p> <ul style="list-style-type: none"> o The tractor and the trailer should be tracked from gate out to gate in using “smart truck” technology. o Reporting (polling) frequency for truck/trailer location should not be more than 15 minutes. o Shippers/carriers should have the ability to “define and monitor” routes and risk areas. The monitoring system should detect when a truck is off-route or nearing a risk area and send an alert to the dispatch center. o “Smart truck” technology should be deployed to remotely monitor trailer “connect” and “disconnect” events. Location polling frequency for a disconnected trailer should be frequent enough to enable quick trailer recovery. o Truck tracking vendors need to deploy TSC-compliant technology and report data in a TSC-compliant manner. <p>TSA’s Tier 1 HSSM compliance requires “smart truck” technology deployment by carriers and the systems to manage data from “smart truck” deployments.</p> <ol style="list-style-type: none"> 1. Truck-mounted GPS receiver and wireless modem (to support vehicle location monitoring). 2. Untethered trailer tracking systems to monitor trailer connect and disconnect events. 3. In-cab and/or remote panic buttons. 4. In-cab device (biometric plus OBC) to prevent unauthorized drivers from driving truck.

TSA's Tier 1 HSSM compliance requires shippers, carriers, and receivers to use the services of truck tracking vendors. Regulations will need to define a "truck tracking vendor" as a regulatory entity and establish performance requirements for truck tracking vendors. Note that TSC systems must accept data feeds from truck tracking vendors and the data submission requirements will need to be developed.

Truck tracking vendors need to modify their "smart truck" technology offerings to meet TSA Tier 1 HSSM regulatory requirements.

Truck tracking vendors need to modify their data reporting systems to feed data to the TSC to meet TSA Tier 1 HSSM regulatory requirements.

Transportation Security Center systems must meet future TSA Tier 1 HSSM regulatory needs.

1. The business processes underlying the TSA Tier 1 HSSM regulatory requirements should be automated with TSC systems serving as the messaging mechanism.
2. Users must be able to enter an electronic manifest (load type/quantity; shipper, carrier and receiver information; ETA).
3. Users must be able to enter primary and alternate routes (e-route).
4. System should automatically monitor route adherence and send alerts when needed.
5. System should monitor shipment chain of custody.
6. System must be able to accept "gate out" and "gate in" notifications.
7. System should be able to alert en-route carriers/drivers that Orange or Red conditions have been implemented by DHS and that alternate routing should be taken.
8. System should be able to accept driver input that the driver is delayed (ETA change) or that the driver is taking an alternate route.

PL 110-53 9/11 Commission Act of 2007 – August 3, 2007

2.5

PL 110-53 contemplates regulations that will have a base set of requirements for shipments of "security sensitive" materials – focusing on those materials subject to TSA (Tier 1) HSSM guidance. This reinforces the conclusion reached in Section 2.4 that the model program regulatory should focus on hazmat carriers hauling materials requiring Tier 1 HSSMs.

PL 110-53 contemplates regulations that will require certain hazmat carriers to deploy "smart truck" technology that will provide:

- o frequent or continuous communications;
- o vehicle position location and tracking capabilities; and
- o a feature that allows a driver of such vehicles to broadcast an emergency distress signal.

At a minimum this means that carriers must install a GPS receiver, wireless modem, panic button and employ a third party tracking vendor. The third party vendor must report vehicle location out to a government tracking center.

PL 110-53 also contemplates additional regulatory requirements including:

- o Sensors to detect device tampering
- o Polling frequency
- o Vehicle immobilization
- o Electronic routes (connotes geo-fence monitoring)

PL 110-53 legitimizes the FMCSA Field Operations Test benefit/cost study as the basis for assessing the cost reasonableness of regulations that would be needed to implement the hazmat tracking requirements of PL 110-53.

Section 1553 of PL 110-53 will require security-sensitive hazmat carriers to develop and follow route plans – possibly electronic route plans. Model regulations should require development and submission of electronic routes to the TSC to enable route monitoring especially since they enable more effective geo-fence functionality.

By virtue of its reference to the TSA Hazmat Truck Security Pilot, PL 110-53 explicitly embraces the conclusion that the technology/systems that are needed to make a hazmat truck tracking center work are feasible and field tested. Refer to Section 4.5 for an analysis of the implications of the TSA Hazmat

Truck Security Pilot program on the design and operation of the Transportation Security Center.

PL 110-53 directs TSA to evaluate the feasibility of vehicle immobilization. The TSA Hazmat Truck Security Pilot did not evaluate vehicle immobilization. However, a FMCSA study on vehicle immobilization systems was completed November 2007.

Section 1553 of PL 110-53 will require security-sensitive hazmat carriers to develop and follow route plans – possibly electronic route plans. The system should be designed to accept an electronic route map by the shipper or carrier and should be designed with route monitoring functionality.

EPA Hazardous Waste Electronic Manifest Initiative 2001 - 2008

2.6

State regulations will need to explicitly allow generators, transporters, and TSDFs to use hazardous waste electronic manifests – current regulations allow only paper manifests.

EPA’s “share-in-savings” business model calls for a private company to build and operate an e-manifest processing center. The company will collect a transaction fee for each hazardous waste electronic manifest it processes. EPA’s transaction fee model should be incorporated into the business model for the Transportation Security Center.

The savings associated with hazardous waste e-manifests easily justify user-based transaction fees to support establishment and operation of an e-manifest processing center.

EPA does not plan to make hazardous waste e-manifest use mandatory. Two implementation problems might arise.

- o E-manifest transaction volume may be low and/or slow growing.
- o A large volume of paper manifests may result – preventing the parties from capturing full e-manifest cost savings.

Hazardous waste e-manifest regulatory fee allocation should reflect the relative e-manifest cost savings of the parties.

- o Generators will save almost \$17/manifest and states will save about \$8/manifest.
- o Waste firms with captive transport vehicles will save about \$50/manifest transaction.

EPA plans to allow an “offeror” (transporter) to sign a manifest on behalf of generator. Model regulations need to factor in the role of offeror, especially in regard to the hazardous waste e-manifest business process.

History shows that generators, transporters and TSDFs will not adopt hazardous waste e-manifests without a financial or regulatory incentive (refer to Ontario’s experience Section 4.7). A simple way to promote e-manifest use is an e-manifest transaction regulatory fee in which paper manifest transactions are assessed a much higher fee than e-manifest transactions.

E-manifest model regulations will require manifests (electronic and paper) to be processed through the Transportation Security Center.

Transportation Security Center systems must be EPA CROMERR-compliant and will operate as a node on EPA’s Central Data Exchange (CDX). CDX requirements will drive system interface design between EPA and the Transportation Security Center.

5. Services-oriented architecture using web services applications
6. Schemas and stylesheets developed in XML
7. User registration, user authentication, execution of electronic signatures
8. SSL-secured HTTP sessions for conducting business transactions

Even if regulatory fees for hazardous waste paper transactions are set higher than e-manifest transactions (to encourage e-manifest use), the need to process potentially large numbers of paper manifests will still exist. A high-speed, non-labor intensive paper manifest system needs to be built.

EPA’s uniform national manifest form simplifies data issues in that states cannot require additional data elements on the form. However, states may have different internal e-manifest business processes that may need to be accommodated. The system will need to be flexible in terms of accommodating different state business processes.

Two different signature ceremonies need to be accommodated in the hazardous waste e-manifest business process.

9. Offeror prepares and signs e-manifest on behalf of waste generator
10. Generator prepares and sign own e-manifest

The hazardous waste e-manifest form needs to be able to accommodate partial form signing. For example, the generator portion of the form needs to be signed and “locked” when the custody of the waste shipment shifts from the generator to the transporter.

In the hazardous waste e-manifest business context, a waste management firm is likely to prepare an e-manifest in advance. At the generator’s location, the transporter would verify waste type and add quantity information to the manifest.

The hazardous waste e-manifest form needs to be able to be rendered on a mobile computing device to support manifest transactions in a field setting. Ideally, transporters will use on-board (or handheld) computers and wireless internet connections to support the generator/transporter e-manifest transaction.

EPA’s e-manifest regulatory approach may create a requirement to accommodate a large volume of paper manifests. Efficiency and processing speed will be critical to operational success. Staffing requirements will also change. Document scanning and data entry – perhaps on a large scale – will be required.

Should hazardous waste route tracking be required by transporters/TSDFs? (This would require transporters to install a GPS receiver and wireless modem on their trucks.)

- o Shipment tracking will strengthen chain of custody control of waste shipments.
- o Transporters will capture positive ROI from “smart truck” technology deployment (refer to Section 4.1)

EPA’s approach to e-manifest implementation may result in slow growth in transaction volume. Low e-manifest transaction volume means lower revenues to the private party operating the e-manifest system. A higher e-manifest transaction processing fee may have to be set to cover fixed costs as transaction volume builds. It is unclear if EPA plans to require States to allow companies to use e-manifests (ie requirement for program delegation). If states self-elect, e-manifest transaction volume will grow slowly.

Alliance for Uniform Hazmat Transportation Procedures, NCSL

2.7

The Alliance has developed an on-line carrier registration system. Section 2.7.2.4 describes the data that Alliance states collect from carriers. This data will supply much (but not all) the data needed from high-risk hazmat carriers to meet TSA Tier 1 HSSM carrier registration. Assuming that Alliance and TSC systems are linked, TSC registration systems could pre-populate on-line forms for Alliance carriers and collect only the incremental data needed for TSC purposes.

The TSC’s registration program should query a carrier’s current status in the Alliance and link to Alliance databases for carrier information as appropriate. TSC’s systems should also query the permit status of a carrier before each gate-out event to ensure the carrier has permit authority to accept the shipment.

The Alliance program and the ACE Truck E-Manifest program should be brought into alignment. The data requirements for carrier registration/permitting and data requirements for a cross-border e-manifest should be reconciled. The ACE data needs are much more expansive than Alliance needs, and for the most part the Alliance dataset will be a subset of the ACE dataset. However, both will need to include additional data elements to meet the need to register “smart truck” devices on carrier vehicles.

Joining an existing state program – like the Alliance – should make adoption of new hazmat and hazardous waste regulations easier in Kentucky.



3.0 Technology Drivers

This section examines technology issues that will drive the design and operation of the Transportation Security Center.¹

Section 3.1 describes “smart truck” technology and how it may be used to protect the nation’s hazmat supply chain. Section 3.2 examines how truck-based asset tracking systems have been substantially enabled by advances in communications technology and the implications of better/cheaper technology on the Transportation Security Center. Section 3.3 describes how video-sharing software is enabling mobile devices such as cell phones to connect field operations with central command centers.

Section 3.4 describes XML messaging standards that have been adopted to support hazmat communications and how those standards will be used to build hazmat tracking systems. Sections 3.4, 3.5, 3.6 and 3.7 explore how web-based services are transforming the way government and industry interact and the implications of that technology on the design and operation of the Transportation Security Center.

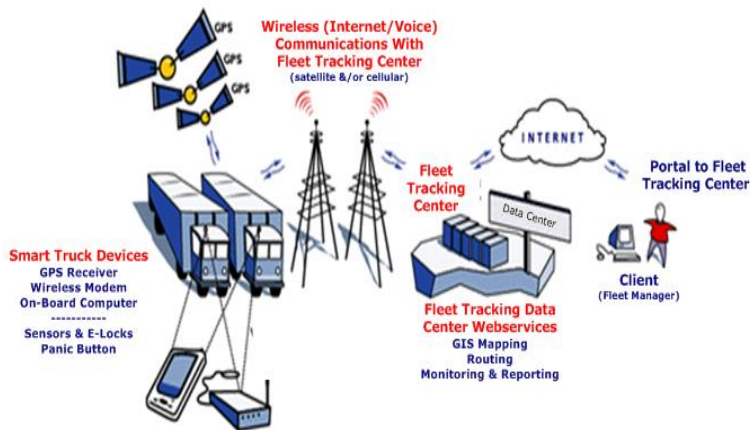
Section 3.8 examines how business rules engines can be built into a powerful tool for modeling and reacting to real-time threats in the hazmat supply chain. Section 3.9 describes systems that have been developed to support operations centers. Section 3.10 describes how agile software development techniques reduce development time and improve software quality.

3.1 “Smart Truck” technology, a core technology component of a hazmat tracking system, is inexpensive and available from numerous vendors.

As illustrated in **Figure 3.1.a**, a typical “smart truck” technology deployment connects truck-mounted smart truck devices to a commercial fleet tracking data center via a wireless modem on the truck. This set-up allows fleet managers to track the location and status of the trucks in their fleets on a real-time basis via an internet connection. Fleet managers use GIS tools (mapping, routing, reporting) and in-cab messaging systems to monitor and manage fleet activity.

Wireless communications systems connect “smart truck” systems with interactive data centers using satellite &/or cellular networks.

Figure 3.1.a Truck-mounted “smart truck” devices are connected to a commercial fleet tracking center by a wireless modem on the truck making the truck a “rolling office”.



An interactive data center lets fleet managers track vehicles on a real-time basis, monitor on-board sensors, and communicate with drivers. GIS tools support mapping and routing.

¹ This section is not an all inclusive analysis of all the “technologies” that will be used in building the Transportation Security Center. It does, however, highlight specific technologies that will serve as core technology components or which have a significant bearing on the design or operation of the Transportation Security Center.

3.1.1 A GPS receiver and wireless modem are core building blocks of a smart truck system.

At the heart of every smart truck system are two components – a GPS receiver and a wireless modem. The GPS receiver provides location data on the truck and the wireless modem is used to report data to a truck tracking vendor. Other components can be added to provide additional functionality.²

A GPS receiver and a wireless modem is the core technology base for a truck-based smart truck technology system.

- **Smart Truck Devices**— As noted above, a smart truck system will minimally involve installation of a GPS satellite receiver and a wireless modem on the truck. The GPS receiver is used to pinpoint the exact physical location of the truck using signals from GPS satellites. The position of the truck is transmitted to a fleet tracking center via the truck's wireless modem over a wireless communications network. Additional devices increase smart truck functionality. Sensors and telemetric devices can monitor a wide variety of truck conditions (brake wear, tire pressure, trailer temperature, engine RPM, etc.), and when connected to an on-board computer (and wireless modem) can supply a continuous stream of live data to fleet managers. Other devices and sensors that are typically connected to an on-board computer include electronic locks, panic buttons, and biometric devices. Like the popular OnStar™ service, smart truck devices connected to an on-board computer can be monitored and/or activated by a remote command center as long as there is a wireless connection to the truck's on-board computer.
- **Wireless Communications (with Global Positioning System)** — A smart truck interacts with the fleet tracking center via wireless modem and a wireless communications network. The truck can use satellite or cellular services for its wireless communications network. Satellite communications networks have traditionally been the choice of long-haul fleet managers, however, systems based on GSM/GPRS cellular wireless networks have experienced tremendous growth. GSM/GPRS cellular systems provide extensive national coverage and are less expensive than satellite communication systems – especially for the needs of mobile service workers. Hybrid satellite/cellular systems that automatically switch between satellite and cellular systems based on network coverage are also available.
- **Fleet Tracking Center Webservices** — Once a truck is connected to the fleet operations center, the truck driver and the fleet manager have access to a rich selection of webservices.

GIS-based tools support sophisticated asset tracking programs.

GIS Mapping Software — The position of a truck is transmitted over a wireless network (cellular or satellite) to a server at a fleet tracking center and then on through to the client (e.g. fleet manager). Usually position/location is reported once/minute or when a truck changes its route or direction. Software at the fleet tracking center uses truck position/location in conjunction with GIS mapping software. The client can view a truck's location on a map on a real-time basis. Also, the software provides the client with the ability to automatically monitor the position/location of trucks and receive reports when trucks deviate from routing set by the client. GIS tools normally available to the client include geo-fencing, geo-routing, geo-zoning, and mapping services.

- **Geo-fencing** of mobile assets to construct a digital, geographic "fence". The client can set "fences" on a map on a truck-specific basis. When the truck "breaks" the fence, the client is automatically notified.
- **Geo-routing** to enforce dangerous route protocols. An electronic buffer is set around a specific road or hauling route. If a truck deviates from its prescribed route, the client is automatically notified.
- **Geo-zoning** a digital geographic boundary of any shape or size around high-risk areas such as tunnels or nuclear facilities. If a truck crosses into the landmarked area, the client is automatically notified.
- **Mapping services** allow the fleet manger access to services such as determining the nearest vehicle to a specific location, viewing the history of a vehicle and polling for current vehicle information.

² This section provides a general overview of smart truck technology. For a more extensive review of smart truck technology refer to - "Homeland Security and the Trucking Industry", July 2005, University of Minnesota and American Transportation Research Institute <http://www.atri-online.org/research/results/Homeland%20Security%20Trucking%20Industry%20ATRI%20Final.pdf>

Intelligent Onboard Computers (OBC) with Wireless Communications — An onboard computer (PDA or fixed device) is a data processing unit that receives and analyzes information from sensors and other devices on the vehicle and then store/present the information in a convenient and easily accessible manner. The OBC is connected to the truck's wireless modem enabling a wireless internet connection on the truck. Various smart truck devices can be connected to the OBC and monitored/controlled by the fleet operations center via the wireless connection. Devices/services that the OBC/wireless setup enables include the following.

- **Mobile worker access to web services and back-office systems.** The OBC/wireless setup essentially allows the truck to become a rolling office. The mobile worker (driver) can use a data terminal or a PDA and the truck's wireless internet connection to tie to web services and corporate back-office systems hosted on servers at the fleet operations center.
 - **Panic buttons.** Panic buttons (dashboard or key fob) allow drivers to send emergency alert messages to the fleet tracking center &/or fleet dispatchers. If used with an OBC, a driver-carried panic button unit can be used to remotely disable the truck.
 - **Vehicle disablement and e-locks.** Connecting the OBC/modem with vehicle operating systems allows dispatcher-initiated remote vehicle shutdowns and trailer door locking/unlocking. Electronic cargo locks (e-locks) prevent unauthorized cargo access.
 - **Security alert notification** Connecting the OBC/modem with vehicle operating systems allows security alerts to be sent to pre-established contacts when onboard sensors, including trailer disconnect, tamper, volumetric, door (e-lock), radiation, temperature are tripped.
 - **Biometrics and smartcards—** These devices are used to positively identify drivers to shippers, consignees, and to their vehicles. Smartcards with predetermined driver-specific information can be used with biometric fingerprint scanners to validate drivers' identities and record drop off, pickup, and truck start up events. When used in the truck, the "bio-login" process sends alerts to dispatchers if an unauthorized person attempts to operate the truck.
- **Routing, Monitoring & Reporting Software** — Software at the fleet operations center allows fleet manager to set up efficient routes and to monitor route compliance. The software also provides detailed operational reports to the fleet manager.
 - **Enhanced route planning** is provided through efficient routing optimization.
 - **Schedule adherence** provides the ability to track how well a vehicle adheres to a planned schedule and issue alerts whenever a vehicle deviates from the path. Users can build schedules using their in-house planning system and upload to the fleet operations center. Notifications such as "behind schedule", or "stopped too long" may be sent to the fleet manager.
 - **Forensic software** provides a log of location, speed, working hours, idle time, alarms and vehicle history.
 - **Command center/ activity reports** automatically access all fleet location and vehicle usage data through detailed activity reports and enable the verification and validation of a wide range of fleet activity from business mileage reporting to "on-the-job times".

A typical smart truck hardware setup (GPS, wireless modem, OBC) costs \$1,000-\$2,500/per truck. Fleet management services using cellular networks cost about \$50/truck/month (higher for satellite based systems).

3.1.2 The truck tracking market is well developed and well served.

Many trucking companies have already installed smart truck fleet tracking systems. Over the past 15 years, for example, Qualcomm has installed its commercial communications and vehicle tracking technology on more than 500,000 commercial vehicles. According to the company, Qualcomm customers include more than 1,500 trucking companies and 34 of the top 35 truckload fleets.

Qualcomm is far from alone in a crowded marketplace. Many firms offer fleet tracking systems and services and some, such as Safefreight Technology, specialize in hazmat fleet tracking/security systems. In addition, companies such as IBM and Savi/Lockheed Martin are integrating smart truck and RFID technology into enterprise supply chain systems to protect hazardous materials shipments (refer to Section 3.2).

Sensors connected to an on-board computer allow fleet managers to track a wide variety of conditions on a truck using browser-based systems.

Smart truck systems are inexpensive to install and operate – about \$2,500/per truck (installation) and \$50/month/truck.

Commercial "smart truck" systems are widely available and inexpensive to deploy. Companies are increasingly integrating smart truck/RFID technologies into enterprise supply chain systems to protect hazmat shipments.

Figure 3.1.b provides an overview of product/service offering from three truck tracking vendors that offer smart truck systems for hazmat shipment tracking. There are many more vendors in the market but this group is representative of smart truck product/service offerings by fleet tracking vendors.

Figure 3.1.b Truck tracking vendors offer an impressive list of smart truck products and services.

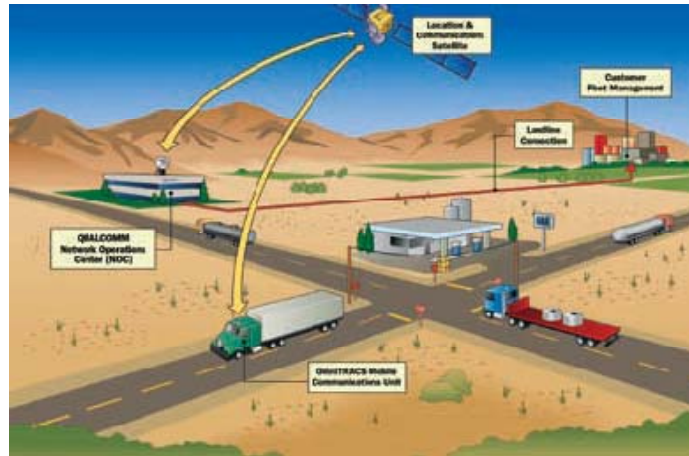
Truck Tracking Vendor	Overview of Truck Tracking Vendor Product/Service Functionality
<p>Magtec Products</p> <p>Calgary, Alberta Willowbrook, IL 888.624.8320</p>	<p>FleetControl™ Solution</p> <ul style="list-style-type: none"> • Vehicle control application • Mobile communication system • M5K™ on-board control system <p>FleetControl™ is a fleet tracking system that offers satellite/cellular network-based applications. At the heart of FleetControl™ is the MK5™ system which allows access to data from smart truck devices via any fixed or web-enabled device. It provides seamless updates to end users on: driver / truck control, asset tracking and security, and safety and risk management. Also enables fuel cost reductions with speed limiters and idle control, and other operational cost reductions.</p> <p>FleetControl™ vehicle security features include the following.</p> <ul style="list-style-type: none"> • Drivers must be authorized to operate vehicle • Fully configurable event notification system • Programmed over-the-air • Complete management of assets by group, by company, by type • Manage driver information and driver authorization codes • Manage maintenance authorization codes, reports, email, SMS notifications on speed thresholds, geo-fence crossover, tamper alarms, panic alerts and vehicle shutdowns • Breadcrumb tracking of assets includes speed, direction and authenticated driver ID recover mode • Remote vehicle shutdown <p>Geo-Fencing; Boundary around asset, route deviations.</p> <p>Keyless Driver Authentication requires a driver to enter a valid driver code before a operating a vehicle. Driver codes can be deleted or changed remotely as required.</p> <p>Tamper Protect™ constantly monitors vehicle systems to detect attempts to bypass the security of the M5K. If tampering is detected, the vehicle is immediately locked down and alert messages are issued – ensuring that a prompt response can occur.</p> <p>Unattended Idle Protect™ (UIP) automatically engages without driver action allowing operators to fully secure the vehicle with the engine running and the key out of the ignition. This allows operators to step away from the vehicle, while remaining confident that their vehicle remains fully protected by the M5K.</p> <p>Timed Maintenance Bypass returns the vehicle to OEM operation for a preset time interval, allowing regular maintenance without disclosing the driver authentication code. The vehicle remains in the maintenance setting until the time interval expires, or the maintenance exit code is entered in the keypad.</p> <p>Acceleration Control System™ (ACS) is unique in the marketplace and a key differentiator between MAGTEC's M5K and any other vehicle immobilization technology. ACS allows dispatch to remotely disable a vehicle by reducing the vehicles' speed in preset increments, bringing it to a safe and controlled stop.</p> <p>Speed and Idle Management™ (SIM) enables the carrier to remotely set, control and geo-fence speed maximums and idle times. SIM maximizes fuel efficiencies resulting in calculable savings in fuel and operational costs along with improving environmental performance.</p> <p>Trailer Tethering (Optional); M5K™ identifies the tractor and TT3 identifies the trailer, when tethered, the TT3 automatically reports to the M5K™.</p> <p>Health Check from Vehicle to Host; Relays current vehicle status and current driver authentication</p> <p>On-Board Event Logging; M5K logs state changes, driver codes and alert triggers</p> <p>Website - http://www.magtecproducts.com/index.html Video: http://www.magtecproducts.com/media/m5k-promo.swf (3:06)</p>

Qualcomm

San Diego, CA
800.348.7227

OmniVisionSM - The OmniVision Transportation service is a comprehensive mobile computing platform designed to enhance the safety, efficiency, and productivity of fleet operations while improving the drivers' in-cab experience. Seamless interoperability with other Qualcomm platforms including OmniTRACS[®] mobile communications system and Asset Management for Trailers and Containers

OmniTRACS[®] is a two-way satellite communications and geolocation trailer tracking technology designed for the over-the-road transport market. On-board the vehicle, the OmniTRACS[®] system sends and receives data from a satellite. The satellite relays information to and from the QUALCOMM Network Operations Centers (NOCs), which communicates with the customer's fleet management center.



Qualcomm's ViaWeb system allows fleet managers internet access to load status and location information 24 hours a day/365 days a year. Using data from the OmniTRACS[®] and OmniExpress solutions, the ViaWeb service provides near real-time information for a fleet's internal and external customers. No additional hardware or software is required, and security is ensured via firewalls and passwords.

QUALCOMM Multiple Access Software System (QMASS) enables automatic data sharing with authorized third parties. Fleets may choose to share specific information—such as vehicle positions—with key partner organizations or customers through QUALCOMM's network operations center.

OmniTRACS[®] also offers a **Security Integration Package**, Qualcomm's high-value or high-risk load monitoring application. It allows companies to customize the frequency of vehicle position reports based on commodity codes, high-risk areas or out-of-route violations. Companies can receive an exception alert if a vehicle has made an unauthorized stop or trailer drop, turns off the truck's ignition prior to delivery or fails to report in to dispatch in keeping with the customer's set parameters. In addition, customized route alerts can be dispatched via pager or e-mail to specified users according to the severity of the exception.

A **Vehicle Immobilization Device (VID)** can be connected to the OmniTRACS[®] mobile communications solution. This enables the authorized operator of the truck to put the vehicle into a "restricted mobility" condition. When used with the Wireless Panic Button—a wireless transmitter for use outside the vehicle—the VID feature increases the security of a truck's load and its driver. In addition to working with the VID, the Wireless Panic Button allows drivers to send emergency notifications with their current locations. Panic message alerts are simultaneously sent to the customer's dispatch and Qualcomm's Network Operations Center.

Other security -related features of Qualcomm's systems include the following.

1. Automated arrival and departing
 - Automatic accurate, timely arrival and departure information
 - Documented proof of on-time arrival and departure
 - Measurement of excessive detention
 - Reporting of unplanned stops
2. Untethered asset (trailer/container) management service
 - Position and event reporting throughout the US, Canada, and Mexico
 - Communicates when connected or disconnected from the tractor
 - Over-the-air firmware upgrades
 - Integration with existing dispatch software
 - Optional door and cargo sensors

	<p>3. Critical event reporting</p> <ul style="list-style-type: none"> • Continuously monitors fleet vehicles for critical events such as hard braking, vehicle yaw and pitch motions, and driver-initiated alerts • Provides driver/truck ID, time/date, position/location, hours-of-service (HOS) compliance, and on-board vehicle sensor and device information such as parking brake status, speed, hard braking deceleration rate and motion stability for potential jackknife or rollover • Provides second-by-second sensor data ranging from five minutes before an event until two minutes afterward • Sends near real-time alerts to safety and fleet managers when critical events occur <p>Website: http://www.qualcomm.com/products_services/mobile_content_services/enterprise/assetmanagement/security.html</p> <p>Video: http://www.qualcomm.com/products_services/mobile_content_services/enterprise/assetmanagement/media/OV-video.htm</p> <p>Product brochures: - OmnitRACS® System for Transportation http://www.qualcomm.com/common/documents/brochures/QUALCOMM-OmnitRACS.pdf - OmnitVision™ System http://www.qualcomm.com/common/documents/brochures/Qualcomm-OmnitVisionTransportation.pdf</p>
<p>Safefreight Technology</p> <p>Edmonton, Alberta Vancouver, WA.</p> <p>780.421.9055</p>	<p>SmartFleet® Manager - Through the SmartFleet® vehicle tracking system, critical location and operating information is gathered through a vehicle-mounted device, communicated wirelessly, and served to Safefreight's customers through Safefreight's vehicle-to-internet application, SmartFleet® Manager. Information can be accessed on-demand from any internet enabled computer or device - any time, from anywhere in the world. Fleet managers can locate and view fleet assets, review historical reports and monitor real-time asset location, condition and security status. Fleet managers can also create and modify business rules for event and alert monitoring and response, asset reporting intervals, geo controls like geofencing and fleet productivity report generation. Features include the following.</p> <ul style="list-style-type: none"> ▪ location reporting ▪ security alerts ▪ security arm/disarm ▪ temperature alert ▪ diagnostic information ▪ remotely managed locking and immobilization ▪ trailer security ▪ two-way messaging ▪ custom reports ▪ forensic tool following accidents or thefts. <p>SecurityGuard™ With the ability to merge cellular and satellite communications with location awareness, asset condition monitoring and control, and many diagnostic sensors, SecurityGuard™ is a platform for real-time tracking, management and security of mobile assets. Additional enhancements can be added to the device, such as sensors (door openings, temperature, seatbelt indicator) and output devices such as sirens, strobe lights and keypad for local alarm activation.</p> <p>EnCompass™ reports the precise location and status of mobile assets at regular intervals in real-time via cellular or satellite networks - providing location speed, time, date, direction of travel and ignition on/off.</p> <p>SafeAlert!™ Fleet emergency response web application delivers information fast, accurately and securely to in-house or third party call center for rapid response. When critical client defined events like unauthorized entry (theft), cargo temperature change and smoke endanger your workforce, cargo or mobile assets, an alert notification is transmitted to pre-defined key personnel or your call center. An automatic text and audible alert notification with asset ID, GPS position, alert details, response procedures and report documentation is served to the customer through this application.</p> <p>Website: http://www.safefreight.com/</p>

3.2 Truck-based asset tracking systems are key components of corporate RFID/supply chain systems.

Smart truck technology deployments save companies money and have the potential to improve hazmat transportation security. Supply chain/RFID technology offers similar benefits.

As described in Section 3.1, smart truck technology connects truck-mounted sensors, GPS receivers, and computers to the internet through wireless modems. The first generation of smart-truck technology relied on satellite networks as the communications medium. Data transfer capacity was limited and expensive, and technology deployment was limited to large interstate carriers. However, since then cellular networks have become pervasive allowing for dramatically cheaper operating costs for smart truck systems. Data capacity has been dramatically enhanced enabling the development of a wide array of sensors and devices that can be placed on the truck.

Radio frequency identification (RFID) systems provide real-time information on the location and state of assets in the supply chain.

Radio frequency identification (RFID) and other automatic identification technologies including electronic seals, biometrics, sensors and GPS satellite location systems are used to provide real-time information on the location and state of assets in the supply chain. In a typical RFID system, individual objects are equipped with a tag. The tag contains a transponder with a digital memory chip that is given a unique electronic identification code. RFID tags can be read-only (passive) or read-write (active). They can be attached to almost anything including pallets, cases of product, vehicles, company assets, high value electronics, and livestock. Radio-frequency waves transfer data between a reader and an RFID tag on a movable item to identify, categorize, and track. The reader initiates tag collection by sending a message to the tag. The tag responds by transmitting its tag ID code to the reader as well as any data collected by the tag. The reader forwards the tag ID/data to a middleware platform that filters and aggregates tag data before it is passed on to system servers and consumed in software applications.

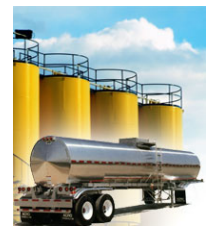
Readers can be either fixed or mobile. Fixed readers can be installed at any location, ideally where the tags frequently pass such as gates or chokepoints, at a point of sale, or in a warehouse. Mobile readers are usually small, handheld devices with a tethered cable or wireless communication. RFID data collection is fast, reliable, and does not require physical sight or contact between reader/scanner and the tagged item. This non-line of sight advantage means that tags can be read through snow, fog, ice, paint, dirt, grime, and other visually and environmentally challenging conditions.

The North American Preclearance and Safety System (NORPASS), pioneered by the **Kentucky Transportation Center**, is an example of an RFID system. NORPASS-enrolled trucks traveling over the Interstate highway system are equipped with RFID tags. As a truck approaches a truck weigh station, sensors in the pavement weigh the truck³ and its tag (truck identity) is interrogated by roadside RFID readers. The truck's identity is used by the NORPASS system to look up the corporate safety record of truck's parent company in the NORPASS database. If the parent company's safety record is acceptable and the truck's weight is within weight limits, the NORPASS system sends a signal back to the truck lighting a green bulb on the dashboard indicating that the truck may bypass the weigh station. A poor safety record or overweight truck causes a red bulb to be lit on the dashboard indicating that the trucker must stop at the weigh station. Bypassing weigh stations save truckers time and money. Almost 60,000 trucks are enrolled in NORPASS in twelve states and two Canadian provinces.



The North American Preclearance and Safety System (NORPASS), pioneered by the Kentucky Transportation Center, is an example of how RFID systems improve transportation efficiencies.

RFID and smart truck technologies are enabling tools for corporate supply chain management (SCM) systems. Leading RFID technology firms such as IBM and Savi have developed tailored SCM applications to support hazmat distribution by chemical and petroleum firms. For example, Savi/Lockheed's *Chemical Custody Supply Chain Solution* enables firms to use smart truck/RFID technology to lower costs and enhance shipment security.⁴



Supply chain/RFID technology offers cost savings and improved hazmat transportation security.

The **Chemical Custody Supply Chain Solution** is a full-featured web-based SCM/RFID application that provides continuous on-line tracking, security monitoring and management of hazardous material containers and their contents from point of origin to destination. Savi/Lockheed designed the Chemical Custody Supply Chain Solution specifically to enhance hazmat supply chain security. The Savi/Lockheed Chemical Chain of Custody Solution can match the physical location of a container and its contents with shipment documents, inventory records, expected routes and destinations, and

³ Trucks are not required to stop or slow down to be weighed. "Weigh in motion" sensors embedded in the pavement record the truck's weight as it passes over; the truck's weight/tag ID is instantly transmitted to the NORPASS system.

⁴ Savi/Lockheed Chemical Chain of Custody Solution; <http://www.savi.com/solutions/so.chem.chain.shtml>

other pertinent information. Using data gleaned from a variety of automatic identification technologies such as RFID, electronic seals, biometrics, sensors, and GPS tracking systems, companies can receive a variety of alerts: if a shipment fails to arrive at a location as expected, if the shipment goes off route, if the shipment was tampered with, if the shipment was handled by someone without proper authority, etc. Alerts can be used to notify security, operational managers, and law enforcement agencies if there is a breach in security protocol.

The Chemical Custody Supply Chain Solution is notable for several reasons.

- *Marketing message.* To date, RFID/SCM vendors have marketed their products by emphasizing the cost savings and service enhancements they offer. With the Chemical Custody Supply Chain Solution, the marketing campaign has emphasized hazmat security as an important, if not the chief, benefit of its product. Savi/Lockheed's message reflects the market's readiness for products and services that address the threat of terrorist actions in the hazmat supply chain. Benefits cited include:
 - reduced liability risk;
 - brand protection;
 - increased security;
 - streamlined operational processes;
 - increased asset utilization and return on assets;
 - reduced asset inventory; and
 - reduced capital investment, lease, rental, and demurrage costs.
- *Chain of custody as a functional focus.* The Chemical Custody Supply Chain Solution was designed to track hazardous materials as custody changed from one party to another. Strict chain of custody maintenance is enabled by the use of electronic records (shipping papers), RFID tags, and GPS tracking systems. Maintenance of chain of custody for waste shipments is a key regulatory objective of EPA's hazardous waste program. Hazardous wastes are a subset of the larger hazmat universe.
- *FMCSA vision relationship/extension.* The Chemical Custody Supply Chain Solution is a step toward implementation of the FMCSA's vision for hazmat security. It is XML-based and data flow to and from a PSRC would be relatively easy to arrange.

3.3 IEEE's 1512 family of XML messaging standards supports intelligent transportation systems.

Clearly defined message sets are essential components in the design and operation of modern, computer-based intelligent transportation systems (ITS). Specifically, a message set provides a series, or set, of individual messages, established in a specific format, for exchanging information on a given topic. An agreed-upon message set with unambiguous definitions is one of the essential standards required to exchange information between ITS systems.

Message sets work in conjunction with data dictionaries that provide the definition and syntax of individual data elements (DEs) that make up the specific message content of a message. In a simple analogy, message sets are the sentences that contain DEs as the individual words. The other standards needed for data exchange provide the actual communications protocols that describe how messages are encoded for transmission, transmitted and then decoded by the receiver.

The IEEE 1512 family of standards supports the exchange of incident-related data between transportation, public safety, and other responding agencies. The IEEE 1512 family consists of a base (or common) standard and several subject-area standards:

- IEEE Std 1512, Common Incident Management Message Sets for Use by Emergency Management Centers is the base standard that defines basic information - such as a description of the incident - that is exchanged for any incident.
- IEEE Std 1512.3, Hazardous Material Incident Management Message Sets for Use by Emergency Management Centers includes messages needed by responders to hazmat spills and other incidents related to commercial vehicles and homeland security.

Savi's sales message reflects the market's readiness for products & services that protect hazmat shipments from terrorists.

The Chemical Custody Supply Chain Solution is consistent with the FMCSA security vision for the hazmat supply chain.

IEEE Standard 1512.3 is an XML messaging standard specifically developed for hazmat shipments and hazmat incidents.

The IEEE 1512 family of standards is used to specify the precise format, data element order, and transactional order of incident management messages passing between agencies that participate in an incident response.

IEEE Standard 1512.3 describes a system of information exchange to be used in a situation where hazardous materials have been released on or near a roadway. The message sets used in the information exchange are primarily for use among hazmat response agencies and between hazmat agencies and any other agencies involved in incident management communications networks.

The message sets in the hazmat Standard work in conjunction with the message sets in the Base Standard. A center will use the Base Standard message sets to transmit information on the type of incident, the location and the center responsible for handling the incident. The message sets defined in the hazmat Standard communicate specific information about any incident involving hazardous materials. The two standards must be used together for useful results.

The following messages, data frames and data elements are part of the IEEE 1512.3 standard.

1. Messages or sets of messages that describe on-site cues about the cargo and/or contents to a remote cargo/contents database, to retrieve more complete data on that cargo and/or contents.
2. Messages or sets of messages that describe the cargo and/or contents to a remote hazard management database, to retrieve data on how to manage any cargo/content-related hazards in the course of the management of the incident. The cargo/contents information can range from quite cursory, such as the first on-site cues, to quite complete, such as the complete information from the shipping papers and even more information from the shipper.
3. Messages or sets of messages that contain information available from telematics messages broadcast from the vehicle. Those messages may be broadcast automatically by the vehicle (triggered by on-board cues indicating an incident, including cues indicating leakage), or upon a command action by the driver of the vehicle.

The IEEE Standard 1512.3 includes XML standards for alerts and messages from smart truck systems.

3.4 Service-oriented architectures integrate business processes.

A business process is a series of logically related activities or tasks performed together to produce a defined set of results. Business processes are often depicted using business process modeling notation (BPMN), a method of illustrating business processes in the form of a diagram similar to a flowchart.

BPMN provides a standard, easy-to-read way to define and analyze business processes and provides a standard notation that is readily understandable by both business analysts and developers. BPMN can also help to ensure that XML documents designed for the execution of diverse business processes can be visualized with a common notation.

A diagram in BPMN is assembled from a small set of core elements, making it easy for technical and non-technical observers to understand the processes involved. Elements are categorized into three major groups called flow objects, connecting objects, and swimlanes. Flow objects, denoted by geometric figures such as circles, rectangles and diamonds, indicate specific events and activities. Flow objects are linked with connecting objects, which appear as solid, dashed or dotted lines that may include arrows to indicate process direction. Swimlanes, so named because of their geometric resemblance to the lane lines on the bottom of a swimming pool, are denoted as solid, straight lines running lengthwise within a rectangle called a pool. The swimlanes organize diverse flow objects into categories having similar functionality.

A business process is a series of logically related activities or tasks performed together to produce a defined set of results.

Service-oriented architecture (SOA) is a methodology for systems development and integration where functionality is grouped around business processes and packaged as interoperable services.

Service-oriented architecture (SOA) is a methodology for systems development and integration where functionality is grouped around business processes and packaged as interoperable services. SOA also describes IT infrastructure which allows different applications to exchange data with one another as they participate in business

processes. The aim is a *loose coupling* of services with operating systems, programming languages and other technologies which underlie applications.

SOA separates functions into distinct units, or services, which are made accessible over a network in order that they can be combined and reused in the production of business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services. SOAs build applications out of software services. Services are intrinsically unassociated units of functionality, which have no calls to each other embedded in them. Instead of services embedding calls to each other in their source code, protocols are defined which describe how one or more services can talk to each other. This architecture then relies on a business process expert to link and sequence services, in a process known as orchestration, to meet a new or existing business system requirement.

In the process of orchestration, relatively large chunks of software functionality (services) are associated in a non-hierarchical arrangement (in contrast to a class hierarchy) by a software engineer, or process engineer, using a special software tool which contains an exhaustive list of all of the services, their characteristics, and a means to record the designer's choices which the designer can manage and the software system can consume and use at run-time.

Underlying and enabling all of this is metadata which is sufficient to describe not only the characteristics of these services, but also the data that drives them. XML has been used extensively in SOA to create data which is wrapped in a description container. Analogously, the services themselves are typically described by WSDL, and communications protocols by SOAP.

SOAP, WSDL, and UDDI are the basic building blocks of web services architecture.

- Simple Object Access Protocol (SOAP) is the XML-based set of rules that govern the call-and-response communication between Web Services-enabled applications. SOAP ensures reliable delivery of Web services messages, and can be seen as the glue that holds Web services together.
- Web Services Description Language (WSDL) is the language that describes the design of a Web service so a client can discover how to invoke and properly use it.
- Universal Description, Discovery, and Integration (UDDI) is the directory standard for registering all of the available Web services currently in use. UDDI is like a Web services phone book, which allows a client to locate a particular Web service that has been published by a provider.

The goal of SOA is to allow fairly large chunks of functionality to be strung together to form ad hoc applications which are built almost entirely from existing software services. The advantage of SOA is that the marginal cost of creating the n-th application is low, as all of the software required already exists to satisfy the requirements of other applications. Only orchestration is required to produce a new application.

3.5 The E-Sign law of 2000 gave electronic transactions the same legal weight as paper-based transactions.

Electronic forms (e-forms) are increasingly replacing inefficient and labor-intensive paper forms in government and industry. The Electronic Signatures in Global and National Commerce Act of 2000, also known as the E-Sign law, gave digital signatures the same legal weight as those signed on paper. The E-Sign Law allowed government and private organizations to place more of their business processes on-line including those that require legally binding signatures. E-Sign has also supported the development of e-forms software to support on-line business transactions.

3.6.1 Electronic (XFML) forms satisfy public and private digital business needs.⁵

⁵ This discussion is based on whitepapers published by IBM describing IBM's Lotus Forms product. Lotus Forms is an e-forms product based on XML/XFDL technology. It has the functionality that would be needed in an XML e-forms product that would meet the business requirements of the hazardous waste e-manifest process. For an overview of e-forms and Lotus Forms: <http://www-01.ibm.com/software/lotus/products/forms/> For an introduction to document security: <http://www-01.ibm.com/support/docview.wss?uid=swg27006755&aid=1>

Forms are vital components of most organizations' business processes. They are the interface point between people and processes, and they supply information to the applications that drive the business. Forms are significant factors in determining how efficiently a process works – and in turn, how smoothly an entire business operates.

Companies such as Adobe, Microsoft, and IBM have developed sophisticated e-forms software to connect documents, people, and business processes. Paul Chan, Program Director for IBM Lotus Forms, offers the following perspective on the use of e-forms in the organization.

"A form is a living, breathing transactional document that interacts with users and information and systems across the enterprise. Today more than 80% of the processes in public and private businesses depend on forms. In each case the form is what initiates the process, it's the vehicle that drives the process through its lifecycle and that kicks off other related processes, and it's the surviving record of all approvals and transactions once the process is complete. It follows that to have any appreciable impact on operational cost and efficiency, an electronic forms solution has to interact with just about every client and every back-end system in the organization."

"(An e-form) is a living, breathing transactional document that interacts with users and information and systems across the enterprise."

Paul Chan, IBM

An e-form is much more than an on-line alternative to a paper form. An e-form is a rich, intelligent, time- and cost-saving front end to an organization's on-line business processes. E-forms software allows organizations to develop secure and intelligent online forms, deploy them to virtually any client, and integrate them with back-end systems and services.

An e-form, often referred to as an **XFML e-form**, is made up of four XML components – 1). Presentation (look & layout); 2). Business logic; 3). Data; and 4). XML attachments. E-forms software provides a single envelope for all four XML components, and one of the most important features of e-forms is that the XML components of the form are not disaggregated as the e-form is processed by the system. For example, when a user applies a digital signature to an e-form, e-form software "locks" the signature to the form exactly as it appeared when the user signed it, and stores that signed version of the form in the database. This is particularly important when multiple & sequential signatures are applied to a form and the form has regulatory or legal importance (i.e. hazardous waste manifest form).

An e-form's XML components are not 'disaggregated' as the e-form is processed through an application's workflow – a major advantage of e-forms.

E-forms serve business processes and the workflow associated with business processes. Dynamic e-forms can be deployed to match workflow needs. Security features keep transactions safe and ensure that data is not tampered with. Entire e-form records may be compressed and stored and data from e-forms flow directly into system databases.

One of the biggest advantages of an online form, compared to a paper form, is the ability to build "intelligence" into the online form. XFML forms can provide sophisticated error checking as the user fills out the form, preventing possible errors (and wasted time as incomplete or erroneous forms are returned to the sender).

Intelligence can be programmed into e-forms to help users avoid errors.

E-forms create great value for organizations. For example, the U.S. Army is in the process of a large-scale project to convert its inventory of 100,000 forms used by 1.4 million people from a paper-based system to an e-forms system using IBM's Workplace Forms™ technology. Internal Army auditors estimate the Army will save \$1.3 billion per year when the project is completed.⁶

3.6.2 Digital signatures ensure document integrity and prevent signature repudiation by system users.

In the on-line environment, document security is critical for applications that focus on the delivery, routing, storing and viewing of documents (e.g. electronic forms). Document security in the on-line environment is a function of a system's ability to maintain document: 1). authentication; 2). authorization; 3). confidentiality; and 4). integrity.

In the on-line environment, document security is a function of:

- authentication;
- confidentiality;
- authorization; and
- integrity.

⁶ <http://www306.ibm.com/software/swnews/swnews.nsf/n/nhan6h9k99?OpenDocument&Site=lotus>

Authentication - How do you know where the document came from?

Authentication involves verification of the identification of a user. This is typically performed at a system level rather than a document level for document access, although there are two points at which a user's identity is critical – when users access documents, and when documents containing digital signatures are assessed. At both points it is critical to ensure that the user is positively identified. System authentication is normally handled by standard web or network-based authentication protocols (i.e., mutual SSL authentication or Windows Network authentication). This type of authentication can enable a system to make authorization decisions. Document-level authentication can also be useful, when the document format permits. Certain types of e-form documents have the capacity to embed decision logic that can detect and respond to an authenticated user via a digital signature or information passed into the document from server-side processes.

A digital signature is created by using a third-party-issued digital certificate. The digital certificate must be provided to the user in such a way as to ensure adequate assurance of the user's actual identity. Many organizations use company-issued cards on which the signing certificate is stored or have security policies in place regarding the issuance of purely electronic certificates. Information from either the certificate or server-side authentication can be used by logic built into the document to restrict access to parts of the document, determine which portions are visible, and block write-access to portions as required if a user is not authenticated properly. Authentication that will be used for multiple levels of access should contain information on access level or role. This information can be embedded within a user's digital certificate or stored on a central server and linked to the user's ID.

Authorization - What permissions does the user have for working with the document?

Authorization is closely linked to authentication, and encompasses the process by which a user or user level is permitted access to different levels or parts of an application. The degree of authorization complexity and security will depend on the application. Typically, applications that define a hierarchical role structure require more complex authorization procedures, in which not only is the user identified, but credentials for the current access level are analyzed also.

Authorization can also occur at various places in an application. Most applications will require authorization for user login, document access, document submission, data queries, and so on. With the exception of user login, most of these authorizations are transparent to the user (single sign-on). Single sign-on systems can be extended to use within the context of the document itself. Document formats that support internal logic can make decisions regarding which sections of a document are available to the user. This is typically accomplished by server-side insertion of session sign-on information into the document or by embedding the document in HTML for portal use. The advantages of in-document authorization are mainly in the area of usability and error reduction. For example, sections of a paper form that are to be filled in by someone with manager credentials can be made read-only or invisible for someone without those credentials. This makes multi-stage documents significantly less error-prone, as well as easier for all users. In-document authorization can also allow for sensitive information to be contained in a document but not available to every user of that document.

Confidentiality - Who is allowed access to the document?

Confidentiality refers to the ability of the system or document to restrict the access of data to authorized users. Data may be in the form of documents or http-based streams (or both). Confidentiality assures that no-one can see or copy the data without the knowledge or permission of the system.

Confidentiality is typically provided through encryption of document or data, and is employed throughout a system. The majority of applications implement transmission confidentiality through the use of secure socket layer (SSL) to encrypt any user-to-server or web services-based communications. As an added layer of confidentiality, it is possible to implement document encryption using a public/private key methodology to ensure that only the owner of the private key can decrypt the document. If the document format supports it, it is possible to store the information regarding permitted access within the document itself.

Integrity - How do you know if the document has been altered?

Integrity refers to the assurance that the document being viewed is exactly the same as the document a user filled out. This is extremely important in documents that are legally binding or have regulatory importance. Document integrity is implemented at the document level but can be checked at various points throughout the system.

Document integrity is typically implemented by use of a digital signature, which is generated by a document hash combined with information from the signer's digital certificate – usually a private key. Biometric information can also be used to generate the digital signature. Many document formats provide only full-document signing capabilities; that is, the user can sign the whole document at once, typically when it has been completed. This type of document integrity is best for single-user documents, since signatures can only be applied to the whole document. Other document formats support multi-stage and overlapping signatures (as well as whole-document signing). A user may fill out part of a form, sign that part, then send the form to another user who can fill out and sign another part of it. The second user's signature can also cover the first user's, which would prevent the first user from subsequently altering anything. This flexibility most closely approaches the process that most forms-based processes naturally follow. It also provides the capability to ensure step-by-step document integrity, rather than simply end-product document integrity.

Digital signatures ensure document integrity, and prevent signature repudiation by system users.

Digital signatures can be used to ensure the integrity of the document by locking all items covered by the signature. Changes to fields or other input items cannot be made once a signature has been applied. Other changes (data, positioning, formatting, visibility, overlap of other elements, etc.) also cannot be made without invalidating that signature on the document. Once the form has been signed by a user, it can also be notarized by an automatic process on the server side for increased assurance of document integrity. Digital signatures also prevent an individual who has signed a document from denying the signature (non-repudiation).

3.6 Internet-based technologies allow the Transportation Security Center to be located anywhere.

Web services are information sources and application components whose functionality and interfaces are exposed to consumers using emerging web technology standards including XML, SOAP, WSDL, and HTTP. In contrast to web sites, web services are offered computer-to-computer, via defined formats and protocols and are capable of processing large amounts of data across the internet.

Using web services, a service provider can be located anywhere there is a suitable internet connection. In addition, voice over internet protocol (VOIP) systems offer location-independent service options that service providers can leverage to complement their web-based services.

- VOIP offers integration with other services available over the internet, including video conversation, message or data file exchange in parallel with the conversation, and audio conferencing.
- VOIP offers advanced telephony features such as call routing, screen pops – all useful in a call center environment. VOIP implementations are easier and cheaper to implement and integrate than traditional telephone/PBX systems.
- Conference calling, call forwarding, automatic redial, and caller ID are zero- or near-zero-cost features that traditional telecommunication companies normally charge extra for.
- VOIP offers secure calls using standardized protocols (such as Secure Real-time Transport Protocol.) Most of the difficulties of creating a secure phone connection over traditional phone lines, like digitizing and digital transmission, are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream.
- VOIP systems are location independent. Only an internet connection is needed to get a connection to a VoIP provider. For instance, call center agents using VoIP phones can work from anywhere with a sufficiently fast and stable internet connection.

Using web services, a service provider can be located almost anywhere. In addition, VOIP systems offer location-independent service options.

3.7 Business rules engines provide sophisticated analyses of market conditions on a dynamic basis.⁷

A business rules engine is a software system that executes one or more business rules in a runtime production environment. The rules might come from regulation ("hazmat carriers without a CDL cannot accept a hazmat shipment"), company policy ("only carriers authorized by the company can accept a hazmat shipment"), or other sources ("carriers of a high-hazard material that cross geofence #267 will trigger a system alert").

Business rule engines allow developers to separate business rules from application code. This is important when rules change often.

Rule engine software is commonly provided as a component of a business rule management system which, among other functions, provides the ability to: register, define, classify, and manage all the rules, verify consistency of rules definitions ("high risk hazmat carriers must report vehicle location every x minutes when it is within y miles of a tunnel" and "high risk hazmat carriers must reporting frequency may not exceed 15 minutes"), define the relationships between different rules, and relate some of these rules to IT applications that are affected or need to enforce one or more of the rules.

In any IT application, business rules change more frequently than the rest of the application code. Rules engines (or inference engines) are the pluggable software components that execute business rules that have been separated from application code as part of a business rules approach. This allows the business users to modify the rules frequently without the need of IT intervention and hence allows the applications to be more adaptable with the dynamic rules.

Business rules produce knowledge; work flows perform business work.

Many organizations' rules efforts combine aspects of what is generally considered work-flow design with traditional rule design. This failure to separate the two approaches can lead to problems with the ability to re-use and control both business rules and workflows. Design approaches that avoid this quandary separate the role of business rules and work flows.

Business rules produce knowledge; work flows perform business work. Concretely, that means that a business rule may do things like detect that a business situation has occurred and raise a business event (typically carried via a messaging infrastructure) or create higher level business knowledge (e.g., evaluating the series of organizational, product, and regulatory-based rules). On the other hand, a work flow would respond to an event by initiating a series of activities.

A business rule will detect that a business situation has occurred and raise a business event (typically carried via a messaging infrastructure). On the other hand, a work flow would respond to an event by initiating a series of activities.

This separation is important because the same business judgment or business event can be reacted to by many different work flows. Embedding the work done in response to rule-driven knowledge creation into the rule itself greatly reduces the ability of business rules to be reused across an organization because it makes them work-flow specific. To deliver this type of architecture it is essential to establish the integration between a BPM (Business Process Management) and BRM (Business Rules Management) platform that is based upon processes responding to events or examining business judgments that are defined by business rules. There are some products in the marketplace that provide this integration natively. In other situations this type of abstraction and integration will have to be developed within a particular project or organization.

Most Java-based rules engines provide a technical call-level interface, based on the JSR-94 application programming interface (API) standard, in order to allow for integration with different applications, and many rule engines allow for service-oriented integrations through Web-based standards such as WSDL and SOAP.

Most rule engines supply the ability to develop a data abstraction that represents the business entities and relationships that rules should be written against. This business entity model can typically be populated from a variety of sources including XML, POJOs, flat files, etc. There is no standard language for writing the rules themselves. Many engines use a Java-like syntax, while some allow the definition of custom business friendly languages.

Most rules engines function as a callable library. However, it is becoming more popular for them to run as a generic process akin to the way that RDBMSs behave. Most engines treat rules as a configuration to be loaded into their process instance, although some are

⁷ This discussion is adapted from the Wikipedia article, *Business Rules Engine* http://en.wikipedia.org/wiki/Rule_engine

actually code generators for the whole rule execution instance and others allow the user to choose.

There are two different classes of rule engines, both of which are usually forward chaining. The first class processes so-called production/inference rules. These types of rules are used to represent behaviors of the type IF condition THEN action. For example, such a rule could answer the question: "Should TSA declare a transportation security incident?" by executing rules of the form "IF some-condition THEN allow-customer-a-mortgage".

The other type of rule engine processes so-called reaction/Event Condition Action rules. The reactive rule engines detect and react to incoming events and process event patterns. For example, a reactive rule engine could be used to alert a watch officer that an unusually high number of dangerous hazmat shipments are moving toward an urban area.

The biggest difference between these types is that production rule engines execute when a user or application invokes them, usually in a stateless manner. A reactive rule engine reacts automatically when events occur, usually in a stateful manner. Many (and indeed most) popular commercial rule engines have both production and reaction rule capabilities, although they might emphasize one class over another. For example, most business rules engines are primarily production rules engines, whereas Complex Event Processing rules engines emphasize reaction rules.

A production rule engine executes when an application invokes it. A reactive rule engine reacts automatically when events occur.

3.8 Web-based crisis information management software supports "virtual" operations centers; enhances communication during an incident.⁸

Information is of little value if it is not collected, evaluated and used in a timely matter. Crisis Information Management Software (CIMS) allows information to be collected from a variety of sources and then be evaluated, shared or viewed by any authorized user. Most CIMS applications are web-based placing integrated crisis information management within reach of most emergency management agencies. Any authorized user with internet access can log into an emergency operations center and gain access to the support offered by the center. This "virtualization" of emergency operations centers dramatically extends their reach and functionality in responding to an incident. The latest versions of some of these applications support handheld devices such as the BlackBerry, Treo/Palm, and the Windows Mobile systems.



Crisis information management software helps run emergency operations centers.

WebEOC™ is one of the leading CIMS packages on the market. It is a web-based information management system that provides a single access point for the collection and dissemination of emergency or event-related information. It was designed to aid decision making by providing authorized users real-time information in a user-friendly format. WebEOC™ can be used during the planning, mitigation, response and recovery phases of any emergency. It can also be used by agencies during day-to-day activities to manage routine, non-emergency related operations.

Information from WebEOC™ can be viewed on individual PC's or displayed onto any number of large screens. It will display text-based lists and reports in conjunction with graphics, maps, video, live TV camera, contact lists and other information needed in an emergency situation. All windows are scalable and movable; and any number of windows can be displayed on any screen, or any window can be displayed across all screens.

"Virtualization" of emergency operations center allows authorized users in the field to gain access to information and incident management tools at the emergency operations center.

WebEOC™ integrates data, video, messaging, and many other types of information. It distributes that information both to individual terminals and to projection screens. It also allows for remote access via the Internet for authorized users. Being able to share real time information with other agencies in an area can allow for more rapid deployment of the regional resources available to emergency managers.

⁸This section highlights a leading CIMS software package, WebEOC™. It was developed at the DOE Savannah River complex and is used by most DOE installations at their primary emergency management tool. The emergency management agencies in Louisville and Lexington both use WebEOC™. Website: <http://www.esi911.com/home/>

MapTac™, a companion software product, can interface with other standard mapping applications and provides a tactical mapping capability that offers common or agency specific mapping views (fire, police, hazmat, etc). WebEOC™ is configurable at the administrator level without need of a programmer. The software can accommodate the Incident Command System (ICS) and FEMA's ESF structure. WebEOC™ offers chronological and categorical status boards of one or multiple incident/events with user configurable screens. Status reports can be directly input by individual responders. It also features a Drill Simulator offering the capability to construct exercises that are scenario based. Real-time links to 911 CAD systems are also possible through WebEOC™.

3.9 Agile software development allows project teams to “develop quickly and deliver often”.⁹

The catch line for Agile software development is “develop quickly, deliver often”. There are a number of agile development methods but all minimize risk by developing software in multiple repetitions (or 'iterations') of short time frames (known as 'timeboxes'). Software developed during one unit of time is referred to as an iteration, which typically lasts from two to four weeks. Each iteration passes through a full software development cycle, including planning, requirements analysis, design, writing unit tests, then coding until the unit tests pass and a working product is finally demonstrated to stakeholders. Documentation is no different from software design and coding. It, too, is produced as required by stakeholders. An iteration may not add enough functionality to warrant releasing the product to market, but the goal is to have an available release (with minimal bugs) at the end of each iteration. At the end of each iteration, stakeholders re-evaluate project priorities with a view to optimizing their return on investment.

Agile methods emphasize face-to-face communication over written documents. Most agile teams are located in a single open office to facilitate such communication with project teams of 5-9 persons. Team composition in an agile project is usually cross-functional and self-organizing without consideration for any existing corporate hierarchy or the corporate roles of team members. No matter what development disciplines are required, at a minimum, every agile team will contain a customer representative. This person is appointed by stakeholders to act on their behalf and makes a personal commitment to being available for developers to answer mid-iteration problem-domain questions. This availability is critical to agile project success.

Part of the Agile framework is routine and formal daily face-to-face communication among team members. This specifically includes the customer representative and any interested stakeholders as observers. Team members report to each other what they did yesterday, what they intend to do today, and what their roadblocks are. This formalized face-to-face communication prevents problems being hidden, provided that someone with corporate influence is always listening.

Agile methods emphasize working software as the primary measure of progress. Combined with the preference for face-to-face communication, agile methods usually produce less written documentation than other methods. In an agile project, documentation, Gantt charts and other project artifacts all rank equally with working product. However, when stakeholders are asked to prioritize deliverables for demonstration at the end of the current iteration, they generally prefer to see working product. Stakeholders are encouraged to prioritize iteration outcomes based exclusively on business value perceived at the beginning of the iteration. If documentation represents higher business value than working software in any particular iteration then stakeholders give it a higher priority than working software. The (cross-functional) development team will accordingly produce that documentation instead of lower priority software.

Agile means being able to quickly change direction. In software development, it requires strong discipline to code for agility. It includes writing tests for functionality before coding. It calls for naming of functionality to exactly match the intent and the terminology of the problem domain. It demands cessation of coding when the tests pass. The sum total of all the disciplines delivers an ability to change direction quickly. New and unexpected functionality required to cope with a sudden change in the business

The agile software development mantra is “develop quickly, deliver often.”

Agile methods emphasize working software as the primary measure of progress. Agile allows project teams to quickly change direction.

⁹ This discussion is adapted from the Wikipedia article, *Agile Software Development*.
http://en.wikipedia.org/wiki/Agile_programming#Principles_behind_agile_methods_.E2.80.94_The_Agile_Manifesto

landscape can be inserted in existing code using test-driven development and all the previous tests will pass or fail to instantly indicate where code needs to be refactored to

stay functional. If functionality is added before it is required then it becomes "dead weight" when refactoring is called for.

The agile methods require the whole team to focus on quality throughout each iteration, which ensures the system is built on a sound foundation. Testing is no longer a phase in the development cycle that begins when development is "frozen." The system under development must be kept in a high-quality, working condition at all times. With software builds and integration taking place on an hourly basis, there is just no time to perform extensive manual tests. To accomplish this goal, the team must commit to automating as much of the testing process as possible. This testing must be done at various levels of the system underdevelopment. Relying solely on testing the GUI level can provide the team with a false sense of security.

Agile methods force quality considerations in each iteration.

Many of the projects using agile methods today are SOA-based projects. Agile methods provide the structure for teams to tackle these challenges by keeping them focused on short-term wins and ensuring the integration of IT with its business counterpart. By tackling the challenges in increments and delivering working functionality more frequently to the project stakeholders, the team begins to gain confidence as they see the solution emerge.

Producing working functionality in steps within complex integration projects may seem impossible. Automation is a critical component in the agile development success. The component-orientation of these projects requires testing at the integration level. In a sense, SOA is gaining success for its ability to provide "agility" to the business. The very nature of SOA is to quickly deliver IT supported change in processes as the business needs and priorities change; a goal similar to agile development methodologies. Iterative, incremental processes are focused on delivering true value to the business in fixed increments of time which creates a culture of success and confidence.

Agile development is consistent with the goals of SOA projects.

The success of an SOA project also depends on the ability to continuously test the system under development. During SOA projects, testing can easily be pushed to the end as teams are consumed with simply finding a solution to the complexity. The knowledge of how the system actually operates comes too late. The goal of an agile development project is to validate at short intervals of the project. By sticking with an agile approach, a much stronger, high-quality solution will emerge.

Through the use of short iterations, teams will begin delivering value to the enterprise immediately. Quality solutions and adaptable architectures will emerge and be delivered with confidence. The working component solutions can be demonstrated to project stakeholders. Collaborative testing tools that support this process are proven and available from commercial vendors. Tools that support project management, system development and customer support are available to suit the needs of various team and technology environments. The key value of the tools should be to provide visibility and demonstrate system integrity as it emerges.

3.10 How will these technology drivers influence the design and operation of the Transportation Security Center?

Figure 3.11.a, summarizes how technology drivers will influence the design and operation of the Transportation Security Center. The yellow-coded portions of the table are focused on hazmat truck tracking. Gold-coded sections focus on hazardous waste electronic manifests and green is relevant to both hazmat and hazardous waste.

Figure 3.11.a Implications of technology drivers on the Transportation Security Center.

Hazmat Truck Tracking	
3.1	The cost of deploying and operating "smart truck" technology systems is low. Clearly, cost-effectiveness will be a key consideration in regulatory decision-making in regards to "smart truck" technology deployment. Section 4.1 goes into detail about the cost/benefit of "smart truck" technology. Refer to Section 4.1 for a more complete analysis of the regulatory implications of
3.2	
3.3	
3.4	

<p>3.8 3.9</p>	<p>"smart truck" technology.</p> <p>The market for smart truck technology is well established (Section 3.1.2). Hazmat carriers use the services of commercial truck tracking vendors (TTV). Truck location data is collected by the TTV and the TTV has the ability to report out vehicle location to the carrier and others. The TTV will become a regulatory character in a hazmat truck tracking regulatory program and will need to have certain regulatory obligations for technology deployment and data reporting.</p> <p>Governmental action agencies need to be able to reach drivers in the event of an incident. The Reality Vision™ product allows a driver to use a cell phone to issue a panic alert (with GPS location), and allows the operations center to take control of the drivers cell phone to gain in-cab awareness. If this capability is needed, regulations need to specify.</p> <p>Hazmat shippers, carriers and TTVs need to use an XML standard interface to submit data and alerts to the TSC. Regulations need to specify the type, frequency, and form of data reporting.</p> <p>The field deployment of "smart truck" technology was evaluated in FMCSA's Field Operations Test (see Section 4.1). TSA's Hazmat Truck Security Pilot evaluated "smart truck" technology in the context of an overall vehicle tracking system. Refer to Section 4 for information on the system design implications of "smart truck" technology.</p> <p>Use a business rules engine to provide a dynamic risk profile of hazmat shipments. Separate business rules from other applications.</p> <p>Use of the Reality Vision™ product will change the workflow for hazmat tracking. It will provide a better capability for the TSC to connect with a driver and determine the seriousness of an incident. The architecture of the system will also change.</p> <p>The Reality Vision™ product will also change the way the TSC and government action agencies might function during an incident. For example, first responders with Reality Vision™ enabled smart phones can send video information from the field and receive information from the TSC on their smart phones.</p> <p>The interface with shippers, carriers, and TTVs should be built using the IEEE XML standards.</p> <p>A business rules engine should be used to create a dynamic population at risk score – individual shipment and system wide.</p> <p>The use of a business rules engine to minimize false positive alarms in the hazmat truck tracking system is critical to containing costs. The more false positives, the greater the staffing level needed.</p>
--------------------	---

Hazardous Waste Electronic Manifest

<p>3.4 3.5 3.6</p>	<p>To meet EPA's Cross Media Environmental Reporting Rule (CROMERR) requirements, hazardous waste e-manifest transactions need to meet a high standard for document security. XFML forms help satisfy EPA's document security needs for authentication, confidentiality, authorization, and integrity. And even though hazmat e-manifest document security needs are not as rigorous, XFML forms provide a high level of functionality for hazmat e-manifest transactions. A key advantage of XFML forms is that the forms can be mated to business processes through workflow software to efficiently serve complex business processes.</p> <p>To meet EPA's e-manifest needs, the TSC will need to serve as a node on EPA's Central Data Exchange.</p> <p>The hazardous waste business process is made up of a number of sub-processes. Consider using SOA.</p> <p>Agile development promotes faster development. TSA and EPA will both benefit if systems are deployed quickly.</p> <p>The TSC will serve as an integrating mechanism for the business processes of hazardous waste and hazmat trading partners. For example, the TSC will tie together the business practices of waste generators and waste management firms. The ability of the TSC to serve these processes will drive up transactional volume. To be most effective, TSC systems should be built on a paradigm of efficient XML messaging.</p>
----------------------------	---

Hazmat Truck Tracking and Hazardous Waste Electronic Manifest

3.6
3.7
3.10

Business process management (BPM) software is used to automate an organization's business processes. The business processes underlying hazmat tracking and e-manifest transactions are complicated and, in large part, driven by regulatory requirements. BPM software allows developers to quickly model and build complicated business processes and to build interfaces with government and private systems.

Section 3.7 highlighted the point that internet technologies enable a web-based service operation anywhere there are suitable internet connections. Somerset's Valley Oak Technology Park has an excellent communications infrastructure in place and could, for example, serve as the location of the TSC.

Agile development promotes faster development. TSA and EPA will both benefit if systems are deployed quickly.

The TSC will serve as an integrating mechanism for the business processes of hazardous waste and hazmat trading partners. For example, the TSC will tie together the business practices of waste generators and waste management firms. The ability of the TSC to serve these processes will drive up transactional volume. To be most effective, TSC systems should be built on a paradigm of efficient XML messaging.



4.0 Lessons Learned (Experience Drivers)

Section 4.0 examines a number of systems and programs that offer valuable lessons for the design and operation of the North American Transportation Security Center. They include the following:

- Federal Motor Carrier Safety Administration's: Hazmat Safety and Security Technology Field Operational Test (Section 4.1); Vehicle Immobilization Systems study (Section 4.2); and Untethered Trailer Tracking Systems study (Section 4.3);
- Singapore's Hazmat Transport Vehicle Tracking System (Section 4.4);
- TSA's Hazmat Truck Security Pilot program (Section 4.5);
- U.S. Customs and Border Protection's ACE truck e-manifest (Section 4.6);
- Ontario Ministry of Environment's Hazardous Waste Information Network (Section 4.7);
- Commission for Environmental Cooperation's vision for a North American waste tracking system (Section 4.8); and
- Taiwan Environmental Protection Administration's Hazardous Waste Shipment Tracking system (Section 4.9).

The project team evaluated the implications of each of the above programs from four perspectives: 1). the model regulatory program the project team is developing; 2). the system design for the Transportation Security Center; 3). the concept of operations plan for the Transportation Security Center; and 4). the implementation plan for the Transportation Security Center.

4.1 U.S. Federal Motor Carrier Safety Administration - Hazardous Materials Safety and Security Technology Field Operational Test

In late 2004, the **Federal Motor Carriers Safety Administration (FMCSA)** completed the Hazardous Materials Safety and Security Technology Field Operational Test (FOT), a study to determine if "smart truck" technology such as GPS tracking, wireless modems, panic buttons, and on-board computers could be used to enhance hazardous materials shipment security.¹

The primary intent of the FOT was to determine the extent to which existing security vulnerabilities in the hazmat supply chain might be reduced by the deployment of "smart truck" technology. The FOT also included a detailed benefit-cost analysis designed to measure the benefit of enhanced security in the hazmat supply chain and to determine which component technologies or integrated systems offer the best mix of improved security balanced against reasonable costs for deployment and operations. In summary, the FOT was designed to answer two questions.

1. Do "smart truck" technologies provide significant macro-level security and safety benefits?
2. If so, are the industry operational efficiency benefits significant enough to drive widespread industry deployment of "smart truck" technology, or is government action warranted to facilitate wide-scale deployment?

4.1.1 How was smart truck technology deployed in the FOT?

The FOT was focused on four different hazmat truck transportation scenarios representing the following industry segments:

- Bulk Petroleum
- Bulk Chemical
- Less-than-Truckload (LTL)
- Truckload Explosives industries



Federal Motor Carrier Safety Administration seminal study – "smart truck" technology and hazmat shipment security (November 2004)

Does "smart truck" provide security benefits?

Does "smart truck" technology save carriers money?

Will carriers voluntarily embrace "smart truck" technology?

¹ Hazardous Materials Safety and Security Technology Field Operational Test Executive Summary: <http://www.fmcsa.dot.gov/safety-security/hazmat/fot/eval-rpt-summary-part4.htm>

A risk and threat assessment methodology was used to identify the types of materials that were of highest concern, as well as the most likely attack scenarios (*theft* of a material, *interception/diversion*, and *legal exploitation*). Specific vulnerabilities were also identified during this phase of the project, which served as the basis for selecting the technologies within each scenario.

The FOT focused on four hazmat/transportation scenarios.

- Bulk petroleum
- Bulk chemical
- Less-than-truckload
- Explosives

As detailed in **Figure 4.1.a**, a wide variety of existing technologies were tested within each scenario. These technologies were integrated based on meeting specific functional requirements set by FMCSA. FMCSA also stipulated that these would need to be commercial off-the-shelf (COTS) technologies, such that they could conceivably be implemented rapidly by the motor carrier industry in the future.

The technologies were grouped together into several packages within each scenario. The grouping assisted in addressing the wide range of vulnerabilities identified in the risk/threat assessment, and for testing several different cost tiers reflecting a range of carrier deployment options based on market conditions. Based on this premise, the various technology components were separated into six technology tiers, ranging from a low-end cost of approximately \$800 per vehicle to a high-end of approximately \$3,500 per vehicle.

The technologies were matched to testing scenarios, which were developed to address the functional requirements and the threats and vulnerabilities identified in the Threat/Risk Assessment. With the overall goal of the FOT being to test technologies

Figure 4.1.a FOT “Smart Truck” Technology Deployment

Scenario	Load Type	“Smart Truck” Components
1	Bulk Fuel Delivery	<ul style="list-style-type: none"> • Wireless Satellite Communication • Global Login • In-Dash Panic Button • Wireless Panic Button • Digital Phone • Terrestrial Communication • On-Board Computer
2	LTL High Hazard	<ul style="list-style-type: none"> • Wireless Satellite Communication • Global Login • In-Dash Panic Button • Wireless Panic Button • Terrestrial Communications
3	Bulk Chemicals	<ul style="list-style-type: none"> • Wireless Satellite Communication • Biometric Authentication • In-Dash Panic Button • Wireless Panic Button • Electronic Supply Chain Manifest
4	Truckload Explosives	<ul style="list-style-type: none"> • Wireless Satellite Communication • Biometric Authentication • In-Dash Panic Button • Wireless Panic Button • Electronic Supply Chain Manifest • On-Board Computer • Wireless Electronic Cargo Seal • Geofencing • Untethered Trailer Tracking

The FOT evaluated different “smart truck” technology suites – 100 trucks were used in the FOT.

installed in **100 vehicles**, each scenario tested a total of **25 vehicles**, with various combinations of technology installed on each vehicle. **Figure 4.1.a** provides a summary of each scenario and the technology components that were tested by scenario.

The cost of deploying “smart truck” technology for each scenario above was calculated as well as the benefit of deployment. Additional information was gathered on such topics as the operational effectiveness of the technology, customer satisfaction, and institutional challenges. For example, drivers were asked about the ease of use of the various technologies, and how adding the technology impacted their daily operations. *Quantitative data* was collected primarily through system-generated archived reports.

The FOT benefit/cost studies focused separately on **operational efficiency** and **security**. In the first case, the study team quantified the operational efficiency benefit of “smart truck” technology deployment. Savings from operational efficiency gains will be important in industry acceptance of “smart truck” technology deployment. In the second case, the study quantified the societal benefit of an enhanced hazmat supply chain through the deployment of “smart truck” technology.

4.1.2 How does “smart truck” technology deployment affect carrier costs?

Some of the technologies tested in the FOT are security-oriented only, and do not contribute to operational efficiency cost savings for carriers (i.e., panic buttons, e-seals). Two technologies – wireless communications and GPS vehicle tracking – created exceptional operational efficiencies for hazmat carriers. Notably, these two core technologies also “enabled” other security technologies. Without the deployment of wireless communications and asset tracking, the study determined that other security technologies would not enhance the security of the hazmat supply chain.

Based on the information collected during the FOT, at the micro or carrier-level, benefits were gained through closer management of assets and personnel. Better management reduced out-of-route miles, enhanced driver productivity by facilitating the monitoring of location and driver work status, and through dynamic routing, potentially realized the opportunities for additional loads. The core mobile communications and asset tracking enabled the motor carriers to monitor their fleet operations both in near real-time and through historic record analysis to set tighter performance measures, and to realign fixed and variable routing decisions.

Figure 4.1.b displays the operational efficiency cost savings that hazmat haulers can be expected to capture from deploying the two core security technologies – wireless communications and GPS vehicle tracking. The operational benefits are estimated to be \$486/truck/month (bulk fuel), \$820/truck/month (LTL-high hazard), \$593/truck/month (bulk chemicals), \$914/truck/month (explosives).

The FOT team completed cost/benefit analyses of “smart truck” technology deployment. The team evaluated:

1. ROI on technology deployment from **operational efficiency** gains; and
2. **security benefits** of technology deployment.

Wireless communications and GPS vehicle tracking is core “smart truck” technology – without them the other technologies do not work.

A basic “smart truck” technology package generates overwhelmingly positive ROI for hazmat carriers due to operational efficiency gains.

As illustrated in Figure 4.1.b, GPS and wireless communications generates \$7,116/truck in annual operational benefits for bulk chemical carriers.

Figure 4.1.b Estimated Monthly Per Truck Operational Benefits by Using Wireless Communications With GPS Vehicle Positioning System

Benefits	Bulk Fuel	LTL – High Hazard	Bulk Chemicals	Truckload Explosives
Reduced Call Stops & Check Calls a. Reduces telecommunications costs b. Increases number of trucks dispatchers handle c. Increases potential number of loads d. Reduces idle time fuel consumption e. Reduces idle time engine wear		\$296 a. \$28 b. \$165 c. \$27 d. \$65 e. \$11	\$253 a. \$19 b. \$122 c. \$37 d. \$65 e. \$11	\$491 a. \$30 b. \$81 c. \$290 d. \$78 e. \$13
Improved Maintenance Scheduling • Reduces maintenance & repair cost • Increases revenue miles by reducing downtime		\$36	\$18	\$37
Reduce Out-Of-Route Mile • Creates savings of line haul variable costs		\$180	\$123	\$116
Improved Vehicle Utilization by Reducing Empty Miles • Increases potential number of trips		\$309	\$199	\$270

Total Monthly Benefit Per Truck	\$486	\$820	\$593	\$914
Total Annual Benefit Per Truck	\$5,832	\$9,840	\$7,116	\$10,968

4.1.3 What is the ROI for “smart truck” technology deployment?

Figure 4.1.c presents the annual cost a hazmat carrier would incur in installing and operating the core smart truck technology package (wireless communications with GPS). The annual costs per truck include the initial purchase of equipment and installation amortized over 3 years plus annual messaging and maintenance service fees.

The choice of terrestrial versus satellite-based systems in **Figure 4.1.c** is based on using the lowest cost service appropriate to the operational characteristics associated with the test scenarios. For example terrestrial is more appropriate for the shorter hauls in more developed areas with good terrestrial coverage associated with the bulk fuel and LTL-Non-Bulk scenarios. The longer hauls in more remote areas characteristic of the Bulk Chemical, LTL-High Hazard and Truckload Explosives operations require the coverage afforded by satellite service.

Figure 4.1.c Per Truck-Specific Technology Costs
(Wireless Communications with GPS Tracking Capabilities)

Item	Purchase Cost Per Truck Terrestrial / Satellite	Annual Cost Per Truck Terrestrial / Satellite (3-year amortization)
Mobile Communications with GPS Tracking Units (Hardware Costs)	\$1,000 / \$2,000	\$336 / \$672
Installation	\$200	\$72
Basic Service (per truck) ²	-	\$600
Maintenance Agreement	-	\$180
Total Per Truck Costs	\$1,200 / \$2,200	\$1,188 / \$1,524

“Smart truck” technology is inexpensive to deploy and use – about \$1200 - \$1500/year/truck. Payback on investment is low and acceptable using the investment criteria used by hazmat carriers.

Figure 4.1.d presents the costs, benefits, benefit-cost ratios and payback periods for smart truck technology investment (wireless communications with GPS) by hazmat haulers. Note that the benefits varied significantly. The lower numbers for annual benefits were supplied by a trade group representing the trucking industry. However, even considering the lower benefit numbers offered by the trucking industry, the payback periods estimated for the high-end satellite-based units are within documented ranges for maximum time period that most motor carriers are willing to accept for return on investment.

Figure 4.1.d. Costs, Benefits, Benefit-Cost Ratios, and Payback Periods by Industry Segment
(Wireless Communications with GPS Tracking Capabilities)

Segment/ Fleet Size	Annual Cost/Truck³	Annual Benefit/Truck	Benefit-Cost Ratio	Payback on Purchase in Months
Bulk Fuel (Terrestrial)	\$1,188	\$5,832	4.9:1	3
LTL-High Hazard (Satellite)	\$1,524	2,352 to \$9,840	1.5:1 to 6.5:1	3 to 17

“Smart truck” technology benefit-cost for hazmat carriers.

- Bulk fuel – 4.9 to 1
- LTL high hazard – 6.5 to 1
- Bulk chemicals – 4.7 to 1
- Explosives – 7.2 to 1

² Monthly service fees cover hourly positioning and base number of messages per unit.

³ Costs include purchase and installation costs amortized over 3 years, plus ongoing messaging and maintenance costs.

Bulk Chemicals (Satellite)	\$1,524	\$1,560 to \$7,116	1.0:1 to 4.7:1	5 to 34
Truckload Explosives (Satellite)	\$1,524	\$1,824 to \$10,968	1.2:1 to 7.2:1	3 to 25

4.1.4 How big is the market for “smart truck” technology deployment?

Figure 4.1.e presents data on current technology deployment levels by hazmat haulers. Almost half of hazmat haulers in the United States have deployed smart truck technology.

Figure 4.1.e “Smart Truck” Technology Deployment Levels

Load Type	New Potential Market	Current Penetration	% Current Penetration	Unrealized Market Potential
Bulk Fuel	111,031 Trucks	51,768 Trucks	47%	59,264 Trucks
LTL-High Hazard	145,184 Trucks	70,779 Trucks	49%	74,405 Trucks
LTL-Non-Bulk	368,380 Trucks	178,926 Trucks	49%	189,454 Trucks
Bulk Chemicals	61,168 Trucks	28,963 Trucks	47%	32,204 Trucks
Truckload Explosives	8,195 Trucks	3,823 Trucks	47%	4,373 Trucks

4.1.5 How will “smart truck” technology deployment affect carrier profits?

If the hazmat trucking industry fully deployed smart truck technology, the industry (at the high end) would have to invest \$543 million and incur annual service fees of \$829 million per year. If the purchase costs were amortized over 3 years, total annual costs (including monthly service fees) would be approximately \$457 million. Offsetting these costs would be increased profitability, estimated to range from \$943 million to \$1.7 billion per year. These estimates are presented in Figure 4.1.f.

Full deployment of “smart truck” technology by hazmat carriers will require a one-time \$543 million investment, but carrier profitability will rise by \$1.7 billion/year.

Figure 4.1.f. Full Deployment Investment - Industry Efficiency Benefit and Cost Estimates/Investments Over 3 Years - Wireless with GPS (In Millions of Dollars)

Load Type	Unrealized Market Potential	Technology Investment	Investment Amortized Over 3 Years	Annual Service Fees	Total Annual Costs	Total Annual Benefits
Bulk Fuel	59,264 Trucks	\$71	\$24	\$46	\$69	\$346
LTL-High Hazard	74,405 Trucks	\$164	\$55	\$57	\$112	\$175 to \$732
LTL-Non-Bulk	189,454 Trucks	\$227	\$76	\$146	\$221	\$364
Bulk Chemicals	32,204 Trucks	\$71	\$24	\$25	\$48	\$50 to \$229
Truckload Explosives	4,373 Trucks	\$10	\$3	\$3	\$7	\$8 to \$48
Totals	359,700 Trucks	\$543	\$181	\$276	\$457	\$943 to \$1,719

4.1.6 What methodology did the FOT project team use to calculate the security benefit of smart truck technology deployment?

The primary objective of the FOT was to determine if smart truck technology could reduce security vulnerabilities in the hazmat supply chain. The FOT also focused on quantifying the societal benefits of enhanced hazmat security.

The FOT analyzed the financial impact of hazmat-based terrorist attacks to calculate the security benefit of “smart truck” technology deployment.

The FOT project team faced two challenges, however, in assessing the societal benefits of smart truck deployment.

1. The project team could not predict how many terrorist attacks might occur in the future.
2. The project team needed to create a methodology to quantify (i.e. monetize) the risk reduction effects of smart truck technology deployment.

The project team used the classic vulnerability assessment equation below in which the term, cost, is the financial impact of hazmat-based terrorist attacks.

$$\text{Cost} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

By applying this formula both before and after the deployment of technologies, the project team determined the likely security impacts of the test technologies and expressed these impacts in monetary terms.

To begin the technology benefits assessment, the FOT project team identified the most likely terrorist attack profiles for each of the four load types (bulk fuel; less-than-truckload high hazard; bulk chemicals; and truckload explosives). The following attack profiles were considered.

- **Theft** is undertaken by means of stealth, deception, or force. Stealth and deception are deterred by detection, while force assumes detection and operates within parameters defined by the time to communicate and mount an interdiction. Stealth, deception, and force also define an escalation path for operational planning purposes.
- **Diversion** is a tactic that results in either theft or interception. The purpose is to create a path to a target opportunity or arrive at a location where control of the cargo by the terrorists can be achieved.
- **Interception** is the "instantaneous" version of theft in that the cargo is released and/or detonated, and ignited while still in control of the shipper/carrier/consignee. Particularly effective when the radius of damage is large, this is potentially the most violent of attack profiles in that it likely involves explosives as the mechanism for effecting material release.

For example, a possible associated attack profile for a bulk fuel shipment may be the use of false manifest to divert the shipment and delivery to a populated area for intentional release.

The FOT evaluated likely attack profiles for the four hazmat loads and established the probability that a given attack profile might be successful.

Once operational scenarios and attack profiles were established, a determination was made of the extent of the threat, or the probability that a given attack scenario may be attempted. This value is a function of terrorist aims and operating procedures. Note that deployment of smart truck technology may make a given attack scenario less desirable relative to others, but the technology would not alter the terrorist overall desire to inflict harm. Therefore, **threat** was held constant throughout the FOT assessment.

After establishing threat values, the FOT project team determined weight and rank of **vulnerabilities**. These vulnerabilities represent the probability that a given attack profile will be successful, given potential weaknesses in the various stages and processes involved in transporting hazardous materials from shipper to consignee. Three vulnerability factors contribute to the potential success of an attack.

- **Chain of Custody** - Protection of the Chain of Custody (CoC) is the ability to ensure that a shipment is in authenticated hands during the entire transportation process. CoC represents the first line of defense allowing positive tracking of the material from the point of origin to the point of delivery. Each shipment type infers a set of procedures that are followed at points where custody must be affirmed or transferred.
- **Access** - If an attacker is unable to gain access by intercepting the CoC, this individual may elect to take forcible measures to gain control of the shipment and acquire access. Access is the ability to get inside of a critical effects perimeter (CEP) on the asset given that it has been identified and intercepted. The CEP is different depending on the threat. For detonation in place, this perimeter can be thousands of feet; for theft, the perimeter may involve cab entry. Access is measured as the probability that the adversary will get inside the CEP for a given shipment type and given threat.
- **Response Time** - Response time is the timeframe that it takes for authorities to identify that a shipment has been seized, mobilize response forces, close on the

asset, and to neutralize the consequence potential. Response time is a function of the level of monitoring, the location and alert posture of response forces, and the ability to track the asset once it has been commandeered.

Figure 4.1.g illustrates the percent reduction in vulnerability from the deployment of smart truck technology by load type. ⁴

The FOT project team next examined the likely **consequence** of success for a given attack profile and hazmat operational scenario. As with the threat element of the vulnerability assessment formula, the consequence of a successful attack was considered to not change as a result of the technology deployment. The "per event" potential consequences of hazmat-based attacks were obtained from a document developed by Battelle for FMCSA that explored the potential economic impacts of

The FOT determined the percent reduction in vulnerability that "smart truck" technology deployment would deliver.

Figure 4.1.g. Percent reduction in overall vulnerability by load type and technology.

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Base (WC + GPS Position)	17%	16%	16%	12%
Base + PSRC	24%	25%	24%	20%
Base + Panic Alert	27%	25%	25%	21%
Base + Vehicle Disabling	26%	27%	26%	19%
Base + Vehicle Disabling + Panic Alert	32%	32%	31%	25%
Base + Panic Alert + Driver ID + ESCM	35%	36%	33%	26%
Base + Vehicle Disabling + Panic Alert + Driver ID	36%	37%	34%	27%

intentional and non-intentional releases of hazardous materials. ⁵ The study examined the potential consequences as measured by:

- Fatalities and injuries.
- Property Damage including damage to the truck, to other involved vehicles, and to other public and private property.
- Product Loss including quantity and value of the load (hazmat) lost during a spill.
- Environmental damage.
- Evacuation - predominantly short-term relocation of people and business operations.
- Cleanup - stopping the spread of a release and removing spilled materials.
- Traffic Delay - additional travel time experienced by the motoring public due to delays caused by the incident.
- Business Disruption - businesses having to reduce or cease operations because the facility is inaccessible, supplies cannot be received, or other constraints imposed by the incident.

The FOT estimated the economic impact of the intentional and non-intentional release of hazardous materials.

⁴ Battelle, *HAZMAT Field Operational Test Task One: Conduct A Risk/Threat Assessment*, Draft Report prepared for the U.S. Department of Transportation (USDOT), Federal Motor Carrier Safety Administration (FMCSA), October 2002. Also, from Battelle, *Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials*, Final Report, prepared for the USDOT and FMCSA, December 2003.

⁵ *Framework for Assessing Safety & Security Incident Consequences for Highway Shipments of Hazardous Materials*, Final Report, Battelle, prepared for the USDOT and FMCSA, December 2003.

Figure 4.1.h illustrates reasonable worst-case consequences of attacks using different types of hazardous materials.

Figure 4.1.h. Reasonable Worst-Case Per Attack Consequences

Hazardous Material Load Type	Reasonable Worst-Case Hazmat Attack Consequences
Bulk Fuel	\$3.7 Billion
Less Than Load High Hazard	\$2.1 Billion
Bulk Chemicals	\$16.3 Billion
Truckload Explosives	\$13.3 Billion

The FMCSA estimates a single hazmat attack can create economic damages of more than \$16 Billion.

To put these consequence numbers into context, two incidents provide examples of the harm that can occur from explosive material delivered in a van or light truck.

- The 1993 New York World Trade Center (WTC) bombing killed six people, injured over 1,000, and resulted in over \$113 million in loss of life and bodily injury, and over \$510 million in insured losses (based on figures from the Federal Emergency Management Agency). Total losses are estimated to be \$623 million.
- The Oklahoma City bombing killed 168 people, injured 601, and resulted in \$560 million in loss of life and bodily injury, and over \$125 million in insured losses. Total losses are estimated to be \$685 million.

Vehicles used in the transportation of hazardous materials typically have much larger capacities than the vehicles used in these two incidents. If these vehicles were used to carry out a terrorist act, the damage would have been far worse. If certain hazardous materials were involved and released in a directed attack, it could result in far greater numbers of casualties and damage to property over a larger area.

Another example of the impacts of directed attacks in the United States, albeit attack(s) using airplanes against buildings as opposed to trucks, is the September 11, 2001 attack(s) on the WTC. The Government Accounting Office (GAO) reviewed eight studies from seven organizations that examined the financial impacts of the 9-11 attack on the World Trade Center.⁶ The GAO concluded that the study conducted by the New York City Partnership and Chamber of Commerce provided the most comprehensive estimates: \$83 billion in 2001 dollars for direct and indirect costs.

The 9/11 attack on the World Trade Center resulted in \$83 billion in direct and indirect costs.

The final activity in the benefits assessment framework was to establish the potential number and type of terrorist attacks expected over the time horizon of 3 future years. Using these incident occurrence estimates with per incident consequence dollar value and the vulnerability reduction estimates, overall reduction in potential impacts (benefits) were estimated for each technology countermeasure for each load type.

4.1.7 What is the security benefit of smart truck technology deployment?

In the preceding section, the following equation for the financial impact of hazmat-based terrorist attacks was presented.

$$\text{Cost} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

Although threat may vary over time and is difficult to predict, in estimating the security benefit, threat is held constant at 100 percent, meaning that there is a 100 percent chance that an attempt will be made to use a hazmat shipment for a terrorist attack. Assuming that threat is a constant, the security benefits of smart truck technology

⁶ U.S. Government Accounting Office, GAO-02-700R, *Impact of Terrorist Attacks on the World Trade Center*, May 29, 2002. The reports that were reviewed were prepared by: the New York City Office of the Comptroller; New York Governor and State Division of the Budget; New York City Partnership and Chamber of Commerce; Fiscal Policy Institute; New York State Senate Finance Committee; Milken Institute; and, New York State Assembly Ways and Means Committee.

deployment can be calculated as the overall vulnerability reduction multiplied by the consequences of a hazmat-based terrorist attack. For example, as illustrated in **Figure 4.1.i**, the security benefit that will be generated if bulk chemical haulers adopt “smart truck” technology (wireless communications, gps, vehicle disabling, panic alert) is calculated as follows:

$$\begin{aligned} \text{Security Benefit} &= \text{Bulk Chemical Consequence} \times \text{Technology Vulnerability Reduction} \\ &= \$16.3 \text{ Billion} \times 31\% \\ &= \$5.1 \text{ Billion Benefit} \end{aligned}$$

Figure 4.1.i. Estimated Security Benefits (In Millions of Dollars)

Technology	Bulk Fuel	LTL	Bulk Chemicals	Truckload Explosives
Base (WC + GPS Position)	\$622	\$348	\$2,581	\$1,657
Base + Panic Alert	\$995	\$529	\$4,058	\$2,822
Base + Vehicle Disabling	\$970	\$573	\$4,278	\$2,556
Base + PSRC	\$908	\$525	\$3,891	\$2,652
Base + Vehicle Disabling + Panic Alert	\$1,207	\$689	\$5,098	\$3,355
Base + Panic Alert + Driver ID + ESCM	\$1,318	\$755	\$5,319	\$3,510
Base + Vehicle Disabling + Panic Alert + Driver ID	\$1,331	\$776	\$5,539	\$3,547

A Public Sector Reporting Center will provide government agencies access to actionable information.

The security benefit of “smart truck” technology deployment is substantial – especially for bulk chemical shipments. For example, security benefits exceeding **\$5 billion** will be captured if trucks carrying bulk chemicals were equipped with , wireless modems, panic alerts, GPS, and remote disabling.

4.1.8 What is the Hazmat Public Sector Reporting Center (PSRC)? What implementation issues are associated with the PSRC?

The FOT examined the potential improvements in public sector response capabilities utilizing a Public Sector Reporting Center (PSRC) as the information collection and dissemination point. The PSRC coordinated information gathered from smart truck technology to create centralized information processing and command and control capabilities.

As a “proof-of-concept” system, the PSRC provides a model for enhanced information exchange between public and private sector hazmat stakeholders by providing law enforcement and emergency response personnel access to accurate, timely, and action-oriented information. As a solution, the PSRC system holds the potential to enable law enforcement and emergency response personnel to respond to intentional and unintentional incidents associated with the transportation of hazardous materials. Three “requirements” for the PSRC were evaluated in the FOT.

Requirement 1. Currently, law enforcement typically relies on information provided by the subject for identification. The individual may choose to identify himself or herself using fraudulent identification credentials. It is difficult to remotely verify an individual’s identity and only sketchy information is available without a reliable means to verify identification. An officer must depend on visual identification to make a decision as to an individual’s identity. In the cases of unauthorized drivers, those individuals might have forged identification to pass themselves off as legitimate drivers.

An electronic manifest (ECSM) would provide law enforcement officials visibility into shipment transactions and better information on driver identity.

The Biometric Login or Global Login provides much more accurate, truthful information on a driver during roadside enforcement actions. With laptop access in remote locations, law enforcement can verify driver identity, and with ESCM capabilities, ensure that the correct driver is associated with the correct vehicle/cargo. ESCM manifests detail the entire supply chain transaction from shipper pickup to consignee delivery. The law enforcement officer can determine who should be in control of a shipment at the point of the remote vehicle stop.

Requirement 2. Currently, law enforcement relies on the motor carrier to provide details for an “off route” or geofence-violating truck. Law enforcement information is only as detailed as what the motor carrier provides. In cases where a carrier has no satellite communications, precise vehicle location is impossible with only a rough estimate based on travel times would be available. For details on cargo contents, without ESCM, law enforcement must contact the motor carrier, who may or may not have precise details on what is being hauled. In some cases, the shipper would have to be contacted by law enforcement for precise cargo contents to determine what real risk is posed by a particular off route or geofence-violating truck, depending on what type of material is being hauled.

An electronic manifest combined with real-time tracking provides law enforcement officials with the information needed to detect when shipments are off route.

Geofence alerts contain a precise location of the alert event. Satellite tracking allows for continuing monitoring a vehicle once an alert is received at an increased positioning rate. The PSRC approach is to provide exception-based off route or Geofence alerts to law enforcement or first responders when there is a real defined emergency. Geofencing technology allows each route to be configured according to each specific shipment type, allowing for a precise risk level to be ascribed to each shipment and route. The PSRC allows for law enforcement or first responders to select what types of alerts to receive, and contact by a certain method (phone, e-mail, fax, page, etc.).

ESCM allows for law enforcement to know what cargo is on what truck when responding to an off route or Geofence alert to better assess risk. There is no need to contact the carrier to obtain load information – the information is contained on the manifest when it is electronically accessed.

The PSRC delivers precise, manageable information to law enforcement and first responders when dealing with off route or geofence violating trucks

Requirement 3. Currently, law enforcement does not receive a real-time “panic alert”. The best law enforcement can hope for is a cell phone call placed after the fact, to describe apparent location and what occurred during the event.

Panic alerts provide precise location information to law enforcement officials in the event of an incident.

Panic Buttons provide an effective way to transmit emergency event information directly to law enforcement through the PSRC. Panic buttons utilize satellite or cellular communications to pinpoint exact location and forward that location information to the PSRC and ultimately to end users such as law enforcement. There is no searching for location information pertaining to an emergency event that requires immediate response to a precise location.

As a proof of concept, the FOT demonstrated the PSRC’s ability to fuse and disseminate critical hazmat information in a timely manner to enhance enforcement response to security events. On a basic level, the PSRC system successfully demonstrated that as a system. The PSRC has the ability to improve:

A PSRC will improve emergency and enforcement response to a hazmat incident.

- the response times for emergency and enforcement personnel to respond to a hazmat security or safety incident through the implementation of these technologies and the reporting center operational concept; and
- the quality of the information provided to first responders through the implementation of these technologies and the reporting center operational concept.

In expanding the PSRC concept to a full deployment scenario, the FOT study concluded that significant institutional/ procedural issues will need to be addressed. Among the more important of these is the administration of information and the notification process, i.e., ensuring that shipment information, alert notification levels (triggers), and key persons to be notified are current and complete.

Figure 4.1.j presents the PSRC vision developed in the FMCSA study. The PSRC concept is sound but as Figure 4.1.j shows, the vision as constructed faces significant implementation issue.



Figure 4.1.j. Implementation issues with the Hazmat PSRC

Hazmat Public Sector Reporting Center	
Vision	Implementation Issues
<ul style="list-style-type: none"> • Hazmat transporters will be equipped with smart truck equipment (GPS devices, computing devices & sensors, wireless modems) and will employ fleet tracking services (voluntary deployment) • Hazmat transporters will voluntarily report the following information to PSRC: <ul style="list-style-type: none"> ○ truck location ○ load information (from e-manifest?) ○ routing information ○ alerts (highjack, spill) • PSRC will be an interactive data center. Data flowing to the PSRC will provide government officials with accurate, timely, and action-oriented information that will allow them to: <ul style="list-style-type: none"> ○ detect suspicious activity (ex. route departure) ○ locate stolen vehicles ○ develop/enforce high-risk hazmat zones ○ remotely disable a vehicle ○ respond quickly and with certainty to an emergency (spill/highjacking) 	<ul style="list-style-type: none"> • The PSRC is dependent on voluntary, wide-scale deployment of smart truck technology by hazmat transporters. <ul style="list-style-type: none"> ○ FMCSA study concluded that despite the clear economic benefit of the technology for hazmat transporters, that technology adoption will be too low to make the PSRC concept work. ○ Ontario's e-manifest experience buttresses FMCSA conclusion about industry behavior. • The PSRC is dependent on voluntary data (location, load) reporting by hazmat transporters. <ul style="list-style-type: none"> ○ Unlikely that industry will be keen to voluntarily report data – same issue as voluntary technology deployment ○ Note industry resistance to State/Federal legislation requiring location reporting • The PSRC concept will fail without long-term funding but the FMCSA study was silent on PSRC funding sources. The federal government will incur a long-term funding obligation unless industry is asked to share the cost. The PSRC, as presented, implies a full-federal, forever-federal funding approach. • The PSRC concept will fail without a regulatory push to stimulate technology deployment and data reporting. <ul style="list-style-type: none"> ○ FMCSA study concluded that government intervention (e.g. regulatory push) is needed to promote smart truck technology adoption. ○ Note Ontario's experience and conclusion that a regulatory push is needed. Note that Singapore's hazmat security program required a coordinated technology/regulatory approach. • The FMCSA study was silent on Federal/State implementation roles and responsibilities but there is an implied federal-lead role. A federal, 'one-size' approach to implementing a PSRC program will not provide authorized States the flexibility they need. <ul style="list-style-type: none"> ○ States have delegated responsibility for managing hazardous materials. Response actions take place at the state/local level. The PSRC does not establish the critical link with state action agencies. ○ Authorized states need flexibility. What works for California or New Jersey may not work for Kentucky or Indiana. • DOT/DHS may miss the opportunity to coordinate with the CPB ACE Truck E-Manifest initiative and with the EPA e-manifest initiative.

4.1.9 What observations did FOT study participants take out of the field experience?

The FOT participants made a number of observations in the field exercise.

- **Driver Communications/Asset Visibility.** The participants concluded that frequency in driver/dispatch communication and asset location visibility are key determinants to shipment security. The participants viewed geofencing and untethered trailer tracking favorably from a security perspective. With user-configured polling frequency, these forms of communication types allowed dispatchers to know the whereabouts of their drivers and assets, and to be alerted in the event of crisis or exceptions to normal operational parameters.
- **Average Polling Rates.** The polling rates for GPS positioning were considered too infrequent to effectively track a vehicle, even at 20-minute average intervals. Much more frequent polling is necessary.

FOT participants concluded that FOT participants viewed panic buttons as valuable; an in-dash and driver-carried panic button should be used.

FOT participants believed vehicle disabling is an important security capability, but worried about implementation. Drivers should be able to disable a truck.

FOT participants viewed the PSRC concept favorably but worried about implementation.

FOT participants saw the operational value of GPS tracking and wireless communications.

- Panic Alerts. Panic alerts were considered valuable as reflected in the large incremental increase in vulnerability reduction, but may be limited in effectiveness for more local (within population areas) hauls where the damage could be done before intervention by enforcement. It was recommended that a driver-carried Panic Button be used in conjunction with in-vehicle Panic Buttons. Dissemination of panic notification should be via multiple modes (e-mail, fax, pager, cell phone, etc.).
- Remote Vehicle Disabling. This was also considered a strong vulnerability reduction technology, but it was recommended that it should be combined with driver-local disabling to be most effective, and not be solely reliant upon dispatcher trigger disablement.
- Electronic Seals and Remote Door Locking. These were considered useful for detecting tampering or providing a hard lockout until dispatch approves a door opening. These devices were not considered appropriate to Bulk Fuel and Bulk Chemical operations. Additionally the E-seal concept was not considered as mature as some of the other technologies; therefore reliability and potential cost were issues.
- The Public Sector Reporting Center. In concept, this item was considered as a strong vulnerability reduction system. In terms of identifying crisis and reducing response time, concerns exist about the potential frequency of false alarms/alerts that would burden public safety agencies, integration with existing systems such as computer-aided dispatch (CAD), and the potential cost of deployment.
- Asset Tracking. The carriers saw GPS tracking as a valuable tool in the recovery of stolen tractors and trailers. A tractor-trailer combination unit is worth more than \$100,000 and cargo loads potentially worth much more.
- Core Technology Package (wireless communications with GPS). The carriers saw a number of benefits to the core technology package in terms of improved management of fleet personnel and assets; reduction in unproductive miles; increased driver and dispatcher productivity; and larger loads. The overall impact of the technologies on the motor carriers was that the technologies required the basic communications and tracking system, and that the carriers would realize additional costs in the concept of enhanced security. In this context, panic alerts and remote door locking capabilities were considered very useful with a willingness of carriers to possibly invest in them.

4.2 The U.S. Federal Motor Carrier Safety Administration - Untethered Trailer Tracking Systems

In late 2004, FMCSA completed the Hazardous Materials Safety and Security Field Operational Test. The FOT included an element to test a basic untethered trailer tracking (UTT) system. This system provided trailer position and identification information to a dispatcher on a regular basis.

FMCSA conducted a Congressionally-mandated study on untethered trailer tracking systems, completing the study December 2005.

The House of Representatives Report 107-722, *Department of Transportation and Related Agencies Appropriations Bill*, directed the FMCSA to conduct further study into UTT systems. According to the report:

"Truck trailers pose a significant potential security threat since they provide an easy means to transport dangerous cargos. In addition, the inability to track freight movements causes inefficiencies in the intermodal freight transportation system, increasing operating costs and congestion, and decreasing safety, economic competitiveness, and air quality. While commercially available technology can track a trailer when it is tethered to a cab, commercially available technologies are needed to track and control an untethered trailer. Within the funds provided for FMCSA's limitation on administrative expenses and high priority initiative program, the Committee has provided the funding to leverage existing technology and develop an untethered trailer tracking and control system that will provide real-time trailer identification, location, geofencing, unscheduled movement notification, door sensors, and alarms."

4.2.1 How do UTT systems work? ⁷

Untethered trailer tracking (UTT) systems are comprised of communications and computer technologies for tracking a trailer when it is connected to and disconnected from a truck tractor. These systems use satellite-tracking Global Positioning System (GPS) technology, supplemented by satellite or cellular communications technologies to monitor and track the locations of trailers. Date and time-stamped position reports with the longitude and latitude of a tracked trailer can be sent to a carrier on a regular, event, or on-demand basis via a website, or they can be downloaded to carrier fleet management systems.

Currently available systems allow carriers the flexibility to input asset management settings for their own operations, such as assigning identification numbers to tracked trailers, determining how alerts are generated, and setting up the time intervals for receiving information. For most systems, the location of a single trailer or multiple trailers can be viewed in a map format that includes historical locations and the most recent location of a trailer in various views, including views of the country, region, city, and street where the trailer is located. Also, trailers can be viewed within a specific distance from a specified landmark, longitude/latitude, or population center. Tabular views of output files can show a carrier's fleet and detailed position history of individual vehicles in transit. Using this information, dispatch, logistics, and management personnel can locate assets, respond to shipping and delivery demands, and identify underutilized trailers.

Some UTT systems may also be configured to establish geo-fence boundaries around individual trailers. A geo-fence is an electronic boundary that a user can create to monitor trailer location and movement. For example, a user could locate a trailer on a map and draw a geo-fence around the trailer position by clicking and dragging a mouse. The geo-fence may be assigned to a trailer or to groups of trailers. Geo-fences may also be removed or inactivated for trailers or groups of trailers at any time. Once the geo-fence is set and configured to provide an alert, the system will send a notification to the user if the trailer crosses the geo-fence boundary. Typically, the system will send an alert when a trailer exits or enters the boundary through an email or pager notification. Several systems also provide event-driven exception reporting. Exception-driven reporting will allow the system to monitor trailer position and check for geo-fence breaks frequently, but only send a message if a geo-fence break is detected. Frequent checking for geo-fence breaks without sending frequent messages lowers messaging costs and increases battery life. Geo-fencing can also be utilized in conjunction with some systems that provide trailer connection and disconnection notification information to the carrier's on-site personnel so that they are aware of this tractor trailer information.

Currently available UTT systems may be integrated with sensors that transmit information back to fleet managers and dispatchers. Various types of sensors are capable of detecting cargo presence, temperature, volume, radiation, gas leaks, motion, and door openings and closings. For example, an ultrasonic cargo sensor can detect the presence of cargo in the trailer by indicating if the trailer is unloaded or loaded. A cargo event is defined as the transition from completely unloaded to partially or completely loaded or vice-versa. The systems can be configured to wake up to check the cargo status at a predefined frequency. Utilizing event-driven exception reporting, a status message is sent only when the cargo status changes.

As another part of the system, a door sensor can monitor an open or closed door event on the trailer. A door event is defined as the transition from open to closed or from closed to open. The trailer door sensor can work in combination with the cargo sensor, so that only those door state changes that might affect cargo are sent to the user. For example, it is possible to configure the system to send door open events if there is cargo in the trailer and to ignore door open events if the trailer is empty.

Most systems integrated with sensors generate trailer position information with every message and status report, which is provided to a fleet manager's or dispatcher's computer. Position information can be user-configured to be generated and sent at predetermined time intervals, and it can also be generated and sent upon demand from

An untethered trailer tracking system is part of an overall "smart truck" technology package. It lets carriers know if an unauthorized disconnection of a trailer has occurred.

Other features can be built into the system including cargo monitoring.

⁷ This overview is taken from FMCSA's description of UTT technology; FMCSA Commercial Motor Vehicle Safety and Security Systems Technology – Untethered Trailer Tracking Systems <http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/untethered-trailer-tracking.htm>

the dispatcher's computer. The position reporting frequency is configurable, and many systems have a store and forward capability, if there is a loss of signal.

In most cases, UTT unit terminals are compact, low-profile, and environmentally rugged enclosures, designed to be easily installed on the top of or inside the trailer. UTT systems require a power source and power management strategy for long periods of inactivity, since trailers may be stored in terminals for long periods of time. Currently available systems can be recharged when the trailer is connected to the tractor via the electrical connector (pin 7 on the J560 7-way connector). Some systems can be recharged via solar cells.

Possible limitations of UTT systems may include a loss of signal, cellular channel traffic overload, or equipment problems, such as limited battery life.

4.2.2 The FMCSA developed functional specifications for UTT systems and conducted a field test of commercial trailer tracking systems.^{8 9}

As directed by Congress, FMCSA administered a pilot test for the development of a UTT system in 2005. The purpose of this pilot was to test a UTT system that met specific functional requirements and could improve the safety and security of trailers and shipments at each phase of its movement – pick up, delivery, receipt, and storage.

Eight functional specifications were developed for UTT systems. The eight specification areas are described below. The functional specifications for each area are listed in **Appendix D**.

- 1. Near real-time trailer identification.** Trailer identification is established via position reports sent from the UTT system terminal on the trailer. The UTT system terminal monitors the Global Positioning System (GPS) for its location, checks other on-board sensors, and sends this information over the air (OTA). The information presented to the user includes the trailer identification number (ID) and trailer type, as well as the user Standard Carrier Alpha Code (SCAC). The user can view the host software to find the latest trailer location and status on a map. Trailer locations are displayed relative to predefined landmarks or street or highway intersections. The trailer status refers primarily to three key pieces of information: whether the trailer has cargo or is empty, whether the door is open or closed, and whether the trailer is connected or disconnected to a tractor. If the latest scheduled report is not sufficiently current, the user can request an update from the UTT system terminal. The request will be answered immediately if the terminal is awake. Otherwise, the request will be queued until the next scheduled wake-up time.
- 2. Time of trailer connection and disconnection.** The time of trailer connection and disconnection refers to the time that a trailer is physically connected or disconnected from a tractor. For example, a trailer is typically disconnected from the tractor when the tractor-trailer arrives at a destination where the trailer may be unloaded while the tractor departs to pick up and move another trailer.
- 3. Trailer location and mapping.** Trailer positions are established via GPS or other locating technology. The UTT system terminal is configurable to wake up to check for positions at user-defined intervals. Once the position has been established, the coordinates are reported to the user visually at the carrier site through a map interface. Although latitude and longitude are provided, the user would normally see the trailer's position on a map with reference to highways, streets, intersections, or user-defined landmarks.
- 4. Geo-fencing.** A geo-fence is an electronic boundary that a user can create to monitor trailer location and movement. Geo-fences may be created, viewed, and edited visually on an interactive map. For example, a user could locate a trailer on a

The FMCSA developed functional specifications for untethered trailer tracking systems and conducted tests of commercial systems.

Geo-fences can be built around a trailer or a geographic area.

⁸Untethered Trailer Tracking and Control System; FMCSA; December 2005
<http://www.fmcsa.dot.gov/facts-research/research-technology/report/untethered-dec05/untethered-dec05.pdf>

⁹ Untethered Trailer Tracking and Control System Operational Requirements Document; FMCSA; August 2005.
<http://www.fmcsa.dot.gov/facts-research/research-technology/report/untethered/untethered-trailer-tracking.pdf>

5. map and draw a geo-fence around the trailer position by clicking and dragging a mouse. The geo-fence may be assigned to a trailer or to groups of trailers. Once the geo-fence is set and configured to provide an alert, the terminal will send a notification to the user if the trailer crosses the geo-fence boundary. The geo-fence will send an alert when a trailer exits or enters the boundary through an email or pager notification. Geo-fences may also be removed or inactivated for trailers or groups of trailers at any time.

The UTT system will provide an on-board geo-fence with event-driven exception reporting. Exception-driven reporting will allow the UTT system to monitor trailer position and check for geo-fence breaks frequently, but send a message only if a geo-fence break is detected. Frequent checking for geo-fence breaks without sending frequent messages lowers messaging costs and increases battery life.

A geo-fence might be used to ensure that a trailer remained in a general area, such as the Los Angeles basin. In this example, the user would create a geo-fence around Los Angeles and then assign that geo-fence to a trailer or group of trailers. If a trailer was taken from the Los Angeles area, an alert would be generated and the user notified. This type of geo-fence might permanently remain in effect if this trailer or group of trailers were meant to stay in that area indefinitely. A geo-fence could also be created around a particular destination, such as a receiving warehouse. When the trailer entered this geo-fence, an alert would be generated so that the user would know that the trailer was delivered within a certain timeframe.

Using the UTT system, a user can set a self-centered geo-fence, which provides a quick way to set a geo-fence without forcing the user to locate the area on the map. A self-centered geo-fence uses the position of the trailer at the time of receiving the "set self-centered geo-fence" command to create the geo-fence boundary. The user does not have to create the geo-fence on a map or choose settings for that geo-fence. As with any geo-fence, an alert will notify the user if the trailer breaks the geo-fence boundary while the geo-fence is active.

Ultrasonic sensors can be used to detect if a trailer is loaded or unloaded.

6. **Trailer cargo sensing.** As a part of the UTT system, an ultrasonic sensor detects the presence of cargo in the trailer by indicating if the trailer is unloaded or loaded. A cargo "event" is defined as the transition from completely unloaded to partially or completely loaded or vice-versa. The UTT system terminal wakes up to check the cargo status at a predefined frequency, and a status message may be sent depending on user-chosen settings. For example, an erroneous detection could occur if a person walks into the trailer at the moment the sensor is taking a reading of cargo status. In this case, assuming the person exits the trailer, a second check would show the true unloaded state of the trailer. Validation of cargo events decreases the probability of erroneous state detections.
7. **Trailer door sensing.** As a part of the UTT system, the trailer door sensor monitors for an open or closed door on the trailer. A door event is defined as the transition from open to closed or from closed to open. The trailer door sensor can work in conjunction with the cargo sensor, so that only those door state changes that might affect cargo are sent to the user. For example, it is possible to configure the system to send door open events if there is cargo in the trailer and to ignore door open events if the trailer is empty.
8. **Alerts.** Alerts are generated by the UTT system host software and presented to the viewer through an alert icon that is displayed near the trailer ID. Alerts are based on a combination of user-preferred settings and events which are generated from the mobile terminal. Alerts are used to notify the user of events, such as geo-fence violations. Alerts can be configured to be forwarded to email or pager addresses.
9. **Software requirements.** Requirements for the software that is visible to the system user are included in this section. The UTT system-provider hosts this software that may be accessed by users through the Internet. Using the software, the user may view information, such as trailer positions and cargo, door, geo-fence, or connection events, or configure settings for the system such as landmarks, trailer groups, and user accounts. Additional software requirements are listed in sections above describing time of trailer connection and disconnection, trailer location and mapping, geo-fencing, alerts, and incorporation of fleet management tools.

4.2.3 What are the benefits/costs of UTT? ¹⁰

Untethered trailer tracking can provide an added measure of efficiency and security to commercial vehicle operations. In the United States, the trucking industry uses approximately three times as many trailers as tractors; therefore, loaded and empty trailers can be subject to both theft and terrorism. Trucking companies often buy excess trailers in order to have empty ones on hand to ensure that their most expensive assets - their tractors - are kept busy, leading to the availability and accessibility of trailers and unattended cargo. Due to a lack of manpower and adequate trailer storage facilities, these trailer stockpiles may be either inaccurately assessed or unknowingly disbursed at various locations, increasing their vulnerability to misuse. When a trailer is removed from its dropped location and erroneously moved or parked, a trucking company typically conducts lengthy searches to locate it. As a result, both inefficient operations and security risks prevail in these situations. To reduce the inefficiencies and vulnerabilities relating to the lack of visibility of trailers and their cargo, UTT tracking systems can provide the location of trailers along with additional information, such as cargo and door status indications, trailer movements, and trailer connections and disconnections.

The FMCSA study described the benefit of untethered trailer tracking systems. Systems cost \$600-\$900/truck to deploy.

Enhanced operational efficiency and security are major benefits of UTT systems. Assuring the location and movement of trailers can improve security and operational efficiency by allowing timely recovery of lost or stolen trailers. Trailer yard operational performance can become more efficient through improved record keeping with the automated processes of these systems, since time is not wasted by manually searching for lost trailers. Technology for tracking trailers enables a quick response to find trailers and a tracking capability for thefts in progress. Trailer tracking also provides information about where a trailer has been and how long it was missing.

Typical operations in trailer yards involve loading cargo in trailers and parking the trailers to await a tractor to haul it away. With cargo sitting unattended, the risk of cargo pilferage from a parked trailer is high in a trailer yard. Thieves or terrorists may steal cargo by entering the yard, accessing parking areas, loading cargo in a waiting truck, and removing it from the site. Cargo may also be falsely obtained by personnel showing apparently legitimate identification and pickup orders. Furthermore, unattended cargo may be damaged or used as a potential hazardous weapon or explosive. By providing information on trailer positions with indications of a trailer's location, movement, and cargo and door status, UTT systems can be utilized to reduce the vulnerabilities relating to the lack of visibility of trailers and their cargo.

The UTT system can also be used to maintain an accurate inventory of cargo and trailers in the yard for secure and efficient operations. Yard operations can be better integrated with dock operations to efficiently transfer and accurately track the processing of both inbound cargo deliveries and outbound shipments, particularly high risk loads. Resulting performance benefits of enhanced cargo operations would be improved on-time deliveries, a reduction in yard congestion, and better cargo theft detection and recovery.

The installed cost of UTT systems varies depending upon the type of technology and various sensors that are included with the system. Most systems are a combination of hardware, software, installation, maintenance/service, and recurring monitoring and use fees. The cost of an UTT system, including software, hardware, antennas and transponders, ranges from approximately \$600 to \$900 for the system with monthly maintenance fees starting at approximately \$12 to \$70 per month per trailer, depending upon the type of plan that is purchased. Some plans include a flat fee, while others are based on a flat fee in addition to per-message or air-time usage fees. This price does not reflect the price of servers and dispatch systems, which can vary depending on the customers. The inclusion of various other sensors to the system incurs additional costs. For example, cargo and door sensors cost approximately \$50 each. The systems can be installed by the manufacturer or experienced technicians utilizing detailed manufacturer guidelines.

¹⁰ FMCSA Commercial Motor Vehicle Safety and Security Systems Technology – Untethered Trailer Tracking Systems
<http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/untethered-trailer-tracking.htm>

4.2.4 Who offers UTT products and services?¹¹

As illustrated in **Figure 4.2.a**, the market for UTT products and services is well served by a number of truck tracking vendors. Note: Figure 4.2.a is not a complete list of UTT vendors.

A number of truck tracking vendors offer commercial untethered trailer tracking systems.

Figure 4.2.a The market for UTT products is served by a number truck tracking vendors.

<p>Fleetilla, Inc. 1745 Fritz Dr. Trenton, MI 48183 Phone: 734-699-6153 www.fleetilla.com</p>	<p>GE - Trailer Fleet Services Phone: 800-333-2030 www.trailerservices.com</p>	<p>Interlink Logistics, Inc. Corporate Headquarters 6658 W. Robinwood Lane Franklin, WI 53132 Phone: 630-258-3078 www.cargotracs.com/truckload.asp</p>	<p>PAR Logistics Management Systems 5152 Commercial Drive East Yorkville, NY 13495 Phone: 315-738-0600 ext: 846 http://www.parlms.com</p>
<p>PeopleNet 1107 Hazeltine Blvd, Suite 350 Chaska, Minnesota 55318 Phone: 888-346-3486 Fax: 952-368-9320 www.peoplenetonline.com</p>	<p>QUALCOMM Incorporated 5775 Morehouse Drive San Diego, CA 92121-1714 Phone: 858-587-1121 www.qualcomm.com</p>	<p>Safefreight Technology (USA) 8000 N.E. Parkway Drive Suite 200 Vancouver, Washington 98662 Phone: 360-256-1280 Fax: 360-397-0167 www.safefreight.com</p>	<p>Skybitz 22455 Davis Drive Suite 100 Sterling, VA 20164 Phone: 703-478-2364 Fax: 703-478-3301 www.skybitz.com</p>

4.3 U.S. Federal Motor Carrier Safety Administration – Vehicle Immobilization Systems

FMCSA's Hazardous Materials Safety and Security Technology Field Operational Test quantified the security costs and benefits of smart truck technology (see Section 4.1). After the FOT, Congress directed FMCSA to undertake the Untethered Trailer Tracking and Control Security project (see Section 4.2). These projects used wireless communication systems and GPS tracking as base technologies and included the wireless transmission of tracking data to law enforcement and emergency responders, in addition to the carrier. It was determined that additional technologies, including panic buttons, driver identification, and vehicle disabling could be built onto the wireless communication system to obtain additional security benefits. In FY 2005, the House of Representatives Conference Report 108-792 directed FMCSA to conduct further testing of smart truck technologies, including vehicle immobilization.

FMCSA conducted a Congressionally-mandated study on vehicle immobilization systems, completing the study November 2007.

4.3.1 What is a vehicle immobilization system?¹²

There are different types of vehicle immobilization systems. Some utilize on-board electronics to immobilize the vehicle's engine or braking system to gradually decelerate a vehicle in transit or prevent its initial operation. Others can be engaged remotely using a combination of on-board computers integrated with wireless communications; or non-remotely, utilizing technologies that the driver, operator, or, in some instances, the vehicle itself could execute locally. The systems can be activated manually or automatically based on pre-programmed security conditions.

Vehicle immobilization systems fall into two categories: 1). remote disabling systems; and 2). non-remote disabling systems.

Remote vehicle disabling systems typically rely on a wireless communication system to provide their basic functionality. They can be integrated with panic buttons and on-board computers requiring user identification and/or password log-ins. For non-remote systems, a keypad or key-fob may be utilized as a part of these systems for arming, disarming, and controlling the security system at the asset itself. Non-remote manual systems can also involve the use of in-cab shut-off devices to other vehicle systems, such as electronic ignitions and air brakes.

¹¹ FMCSA Commercial Motor Vehicle Safety and Security Systems Technology – Untethered Trailer Tracking Systems
<http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/untethered-trailer-tracking.htm>

¹² The sections is taken from the overview of vehicle disabling systems on the Federal Motor Carrier Safety Administration Website;
<http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/vehicle-disabling.htm>

4.3.1.1 Remote disabling systems enable a control center to prevent a truck from being used by an unauthorized driver or to stop a moving truck.

A remote disabling system enables a distant control center to stop a moving truck.

Remote vehicle disabling systems provide authorized users at remote locations such as an operations center the ability to prevent an engine from starting, prevent movement of a vehicle, and to stop or slow a moving vehicle. Remote disabling allows a dispatcher or other authorized personnel to gradually decelerate a vehicle by downshifting, limiting the throttle capability, or bleeding air from the braking system from a remote location. Some of these systems provide advance notification to the driver that the vehicle disabling is about to occur. After stopping a vehicle, some systems will lock the vehicle's brakes or will not allow the vehicle's engine to be restarted within a certain timeframe.

Remote disabling systems can also be integrated into a remote panic and emergency notification system. In an emergency, a driver can send an emergency alert by pressing a panic button on the dashboard, or by using a key-fob panic button if the driver is within close proximity of the truck. Then, the carrier or other approved organization can be remotely alerted to allow a dispatcher or other authorized personnel to evaluate the situation, communicate with the driver, and/or potentially disable the vehicle.

4.3.1.2 Non-remote disabling systems enable authorized drivers to stop a moving truck; prevents unauthorized drivers from driving the truck.

Non-remote vehicle disabling systems provide authorized users the ability to restrict or prevent vehicle operation in three ways: through the use of wireless technology when they are near the vehicle; through on-board actions by the driver/operator; or through a combination of both. Non-remote vehicle disabling systems include driver identification authentication technologies, tamper detection alerts, brake locks, and emergency notification panic buttons for disabling the truck in case of an emergency or other event.

A non-remote disabling system prevents unauthorized drivers from starting a truck and enables a driver to stop a hijacked truck.

A single sign-on module is utilized for driver authentication in order to initiate the operation of a vehicle. The driver uses passwords, pin numbers, or biometrics to start the vehicle and to access other on-board wireless communications applications. All activities related to the use of the vehicle are associated with the driver signed-in at the time. This information can be used for dispatch, driver performance, and driver log purposes.

Several different types of technologies can be used to non-remotely disable a vehicle. Panic buttons carried by the driver or within reach of the driver inside the vehicle can be activated to disable a vehicle or send out an emergency notification. Electronic ignition systems allow the driver to automatically activate the system when the key is removed from the ignition and reactivate the system when the key is replaced into the ignition. A relatively low-cost means of vehicle disabling is the utilization of a brake lock device to prevent the movement of the vehicle. A brake lock device shuts down the air line from the tractor to the air brakes in the tractor (and if hooked up, to the trailer). Release of the brake lock system is the only way to move the vehicle.

4.3.2 The FMCSA evaluated vehicle immobilization systems and developed functional requirements.

The FMCSA evaluated commercial vehicle immobilization systems and developed functional requirements.

Important components of vehicle disabling systems are hardware mechanisms that restrict vehicle use. Some are on-board computer technologies that identify the driver to allow authorized use while preventing unauthorized use. Others utilize mobile communication technologies that allow a remote dispatcher or other operator to communicate with the driver and/or the vehicle, and if necessary, activate the vehicle disabling system.

Driver authentication is a vital part of many vehicle disabling systems. Intelligent on-board computers can be utilized for driver identification through global login access where a driver enters login information into a cab-based interface. Similar to a username and password on a computer system, global login is an authentication feature of some wireless communications systems. Through the use of a driver login process, the login information (user ID and password) entered into the truck-based interface by the driver is verified by preset procedures both locally on the vehicle and over the air using the wireless communication system. If this verification fails, various configurable alerts and resulting actions can be triggered up to and including vehicle disabling with the aid of an on-board computer.

Other authentication technologies utilized in several vehicle disabling systems range from PIN number entry to biometric-based systems. The most common biometric-based technologies for vehicle disabling utilize driver fingerprints. If the driver's fingerprint matches the fingerprint information on a biometric smart card carried by the driver, then the driver is verified and able to start the vehicle. If a match is not made, the vehicle cannot be started and the fleet dispatcher is typically notified of the failed attempt.

Vehicle disabling systems can be integrated with many on-board wireless communications systems that include other features, such as door sensors, cargo sensors, temperature sensors, electronic cargo seals, and trailer connection and disconnection systems. For example, if an on-board computer system detects a loss of signal from the communication network or tampering of electronic cargo seals, a pre-determined vehicle disabling protocol can be initiated.

Additional monitoring processes using on-board sensors that detect changes in load volume, door status, exposure to radiation, or temperature can generate a security alert notification that will trigger a vehicle disabling protocol. In vehicles that monitor trailer information, a vehicle disabling protocol can be prompted when a trailer has been disconnected from its assigned tractor or when a trailer door lock system has been violated.

Vehicle disabling protocols can also be activated by critical changes in the status of important vehicle systems. Since on-board computers monitor processes such as coolant temperature and engine oil pressure, a message can be sent to the driver and dispatcher about these conditions alerting them that systems are at unsafe levels. Then, a vehicle can be prevented from starting if unsafe system parameters are discovered prior to vehicle usage. Carriers with refrigerated units (reefers) are significant users of this feature.

Vehicle disabling can be utilized by authorized personnel with a wireless communication system's geo-fencing feature. Dispatchers or fleet operators can create a geo-fence or defined electronic boundary made up of geo-coded points for particular vehicles or routes. If a vehicle enters a restricted geo-fenced area, or exits the defined areas, the dispatcher or fleet operator can be alerted to take necessary actions to secure the vehicle. Currently, no systems available in the U.S. have the capability of engaging automatic vehicle disablement for geo-fence violations. Singapore's Hazmat Transport Vehicle Tracking System does, however, have the ability to automatically immobilize vehicles with geo-fence violations (see Section 4.4).

A study conducted by Oak Ridge National Laboratory for the FMCSA sorted vehicle immobilization technologies into two categories: 1). Vehicle Disabling Technologies (VDTs); and 2). Vehicle Shutdown Technologies (VSTs). VDTs are immobilization technologies that impede **restarting** a vehicle. They can be activated when the vehicle is moving or stationary, but the VDT will only immobilize the vehicle the next time an attempt is made to start it. VSTs, on the other hand, are technologies that cause a vehicle to **lose power while it is moving** and will cause it to eventually come to a stop, as well as impede the restarting of the vehicle after the technology has been triggered. While there are VIT systems that are composed only of a VDT, those that have vehicle shutdown capabilities always have vehicle disabling capabilities as well. ¹³

Figure 4.3.a illustrates the technology components of VSTs and VDTs.

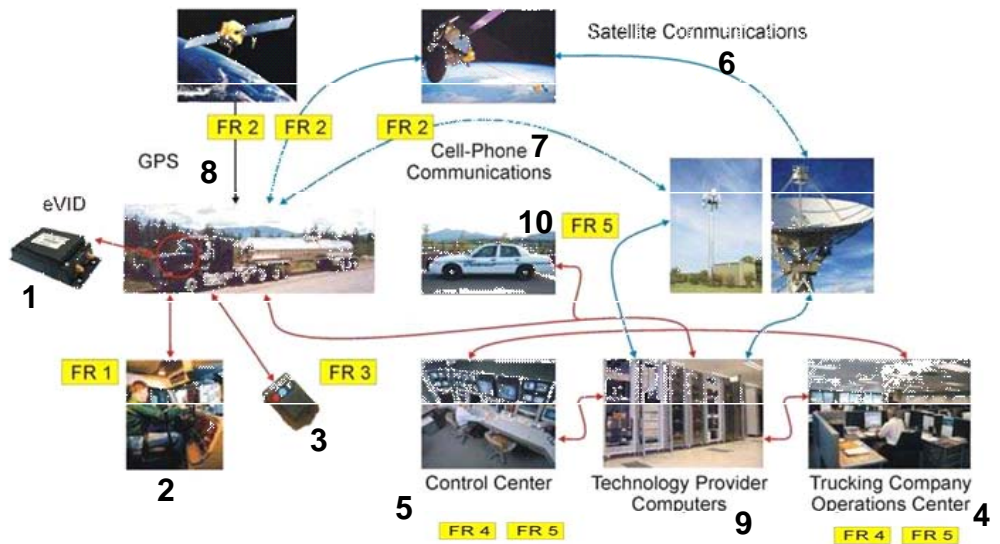
At the core of most vehicle immobilization systems is an electronic vehicle immobilization device (eVID), (Item 1 in Figure 4.3.a) mounted somewhere in the engine compartment of the equipped vehicle. This device can be activated remotely and/or locally to impair the performance of the vehicle via acceleration control, throttle reduction, power reduction or engine shutdown.

Oak Ridge National Laboratory conducted a field evaluation of commercial immobilization systems.

At the core of a vehicle immobilization system is an electronic vehicle immobilization device (eVID).

¹³ The remainder of this subsection is taken from Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement; FMCSA; November 2007 www.fmcsa.dot.gov/facts-research/research-technology/report/VIT-Best-Practices-Law-Enforcement-Nov2007.pdf

Figure 4.3.a Technology components of a vehicle immobilization system.



Usually the default mode of the eVID is “active.” That is, vehicles equipped with an eVID device cannot be started until the eVID is deactivated. The deactivation of the device can be achieved through different means (Item 2 in Figure 4.3.a) which range from keypads—the most common, where the driver enters a predefined code—to swipe cards and RFID (Radio Frequency Identification) tokens, up to biometric devices. Usually, the eVID is activated automatically when the driver shuts down the engine, but it can also be triggered when one of the cabin doors is opened while the engine is running (hijack prevention mode).

The eVID can be activated locally by the driver of a vehicle by use of a key fob.

Outside the cabin, with the engine idling, the eVID can be activated locally (i.e., at a short range) by the driver of the vehicle. This is done through a key fob device (Item 3 in Figure 4.3.a) similar to those used to lock/unlock the doors of passenger cars, but usually requiring two buttons to be pressed at the same time to avoid unintentionally triggering the device. The eVID can also be activate remotely by the dispatcher (Item 4 in Figure 4.3.a) or the technology provider (Item 5 in Figure 4.3.a) if the vehicle is equipped with a wireless communication system, generally satellite (Item 6 in Figure 4.3.a) or cellular communications (Item 7 in Figure 4.3.a), or both. This remote activation also requires a GPS device (Item 8 in Figure 4.3.a) that provides location information for the vehicle.

When activated, the system forwards the vehicle’s location and eVID status to the technology provider’s computers (Item 9 in Figure 4.3.a) using the available communication links (Items 6 or 7 in Figure 4.3.a). Conversely, from the technology provider’s computers and using the same communication links, messages can be sent to the eVID, including those that initiate the shutdown of the vehicle while it is moving.

For the case of a local vehicle disablement (for example, when the eVID enters into a tampering mode after a given number of authentication attempts have been made and failed), the device generally disables the vehicle without waiting to receive a message from the central computers (i.e., the decision is made at the device level on the truck). However, the device sends a message to the technology provider’s computers indicating the problem at hand (in the previous example, conveying that the device has entered into a tampering mode). In some cases, this message is immediately forwarded to the owner of the vehicle through e-mails or phone messages, so the trucking company can take some action (e.g., contacting the driver to determine the nature of the problem). In other instances, the vendor’s control center manages the problem directly and, subsequently, notifies the owner.

Two different models for vehicle shutdown were described in the study. In the first model, the trucking company's operation center (Item 4 in Figure 4.3.a) has direct access to the eVID (Item 1 in Figure 4.3.a) through the technology provider's computers (Item 9 in Figure 4.3.a) and the available communication links (Items 6 and/or 7 in Figure 4.3.a). The trucking company can then send a message to the eVID that initiates the shutdown (or disablement) process without any other exogenous intervention. The second model adds a technology provider's control center (Item 5 in Figure 4.3.a), which is the one that ultimately sends the message to the eVID to start the shutdown process. In this model, the technology provider's control center identifies the location of the vehicle in distress (Item 8 in Figure 4.3.a) and contacts the law enforcement organization with jurisdiction in that area. The shutdown process is initiated only when law enforcement personnel (Item 10 in Figure 4.3.a) are in visual contact with the truck and when they determine that is safe to do so. Of course, this involvement of law enforcement personnel is also possible in the first model, although it is a cumbersome process for the trucking company since it would have to have up-to-date contact information for all the law enforcement jurisdictions in the country.

The FMCSA identified five functional requirements for vehicle immobilization systems.

For purposes of the project study, FMCSA identified five functional requirements (FRs) of interest for VITs.

- FR1: Vehicle disablement if the vehicle senses an unauthorized driver
- FR2: Vehicle disablement/shutdown in the event of a loss of signal
- FR3: Remote vehicle disablement/shutdown by the driver
- FR4: Remote vehicle shutdown by the dispatcher
- FR5: Remote vehicle shutdown by law enforcement

Functional requirement 1 falls into what has been defined in this document as a VDT, while FRs 4 and 5 fall under the VST umbrella. FRs 2 and 3 would be applicable to both VDTs and VSTs, depending on whether the vehicle is stationary or moving.

The five functional requirements are mapped onto Figure 4.3.a. While all of the FRs involve the eVID in this generic VIT system, FR1 is restricted to the truck cabin, the driver, and the driver's interaction with the vehicle immobilization device. Notice that this particular FR can also be satisfied by means other than an eVID; that is, there are mechanical (e.g., brake locks) and other types of devices that can make the vehicle undrivable unless the device is disengaged.

Functional requirement 2 implies the activation of the eVID when one or more of the communication links, either GPS or data transfer, become unavailable for a given period of time. In general, the VIT systems that satisfy this FR allow the user to define the interval of time that needs to elapse before a loss of signal causes a vehicle shutdown. Loss of signal can also produce a vehicle disablement if, for example, a communication wire (e.g., antenna wire) is physically severed or even if somebody tampers with the antenna itself (e.g., covers the antenna with a metal dome) while the truck is idling. Remote disablement/shutdown by the driver (FR3) is accomplished, in general, by a key fob device that allows that driver to send a short range wireless message to the eVID for its activation. This can be achieved while the vehicle is idling (i.e., vehicle disablement) or if someone commandeers the vehicle while the driver is away but at a short range (i.e., vehicle shutdown), such is the case of a vehicle theft at a truck stop.

While the first three functional requirements involve VIT system components that are on the vehicle itself (e.g., in-cabin driver authentication devices for FR1, and antennas and communication systems for FR2) or at a very short distance (e.g., key fobs carried by drivers for FR3), FRs 4 and 5 involve VIT system components that can be located anywhere in the country. A remote vehicle shutdown relies on spatial information regarding the location of that vehicle and bi-directional communication links between centralized computers and the onboard eVID. Those computers can be accessed by an external control center and/or by the trucking company dispatcher. By mapping the vehicle's location information provided by the GPS device, it is possible to determine safe places to initiate the shutdown process or to provide information to law enforcement at the scene to identify the vehicle that is about to be shutdown. The bidirectional communication links with the vehicle serve to receive this spatial information and to send a message to the eVID to initiate the shutdown process.

4.3.3 What are the benefits/costs of vehicle immobilization?¹⁴

The FMCSA study described the benefit of vehicle immobilization systems.

Depending on the actual vehicle disabling technologies utilized, fleet operators can have additional connectivity and communication with their drivers and vehicles compared with fleets not utilizing such technologies. When vehicle disabling systems are integrated with on-board communications and tracking systems, fleet managers can actively monitor security parameters, vehicle routes, performance, maintenance, and fuel usage—whether the vehicles are running locally or on a long-haul. These monitoring capabilities provide operational efficiency benefits for fleet management optimization by providing information about vehicle operation from origin to destination.

Vehicle disabling systems can improve secure operations of carriers who haul high-value or high-risk cargo, such as hazardous materials. Access can be limited to authorized drivers by dispatchers or fleet managers who can manage driver authentication codes and truck identifications, change codes over the air, and disable the vehicle, if necessary. To help prevent theft, a valid driver authentication code can be required before a vehicle can be started or moved. Also, if there is tampering with any integrated security device or fleet management system, the vehicle can be placed in a secure state and an alert can be sent over the air to the carrier. Carriers can also change driver authentication codes and secure a vehicle if a driver suddenly leaves the company, but still has access to the vehicle. The capability to disable the vehicle over the air is also available if dispatchers become aware of a stolen or hijacked vehicle. Even if a truck is moving, the vehicle's speed can be gradually reduced to allow the vehicle to be brought to a safe and controlled stop.

Technologies, such as ignition locks and brake locks can also be used to minimize vehicle theft by prohibiting vehicle movement. These security devices are permanently installed in the vehicle, and they must be utilized in order to operate the vehicle.

The cost of vehicle disabling systems depends upon the type of system installed (i.e., a simple on-board system versus a multi-functional system), the number of systems purchased, and the type of installation required. The costs for less complex on-board systems (such as an ignition lock or brake lock) range from under \$100 to over \$300 per unit, plus installation costs. Installation for these units could be done by a local technician.

The incremental cost of a vehicle immobilization system (on top of core "smart truck" system) is \$500 - \$700/truck.

The costs for basic, non-wireless driver authentication systems utilizing keypad entry range from approximately \$500 to \$700 per vehicle, plus installation costs. Installation for some of these units could be completed by a local technician.

The costs for systems integrated with on-board wireless communications and multi-functional features range from approximately \$2,000 to over \$3,000 per vehicle, plus installation costs. Installation for some of these systems can be completed by a trained technician who is familiar with the technology. However, for technical and/or security reasons, some systems require manufacturer installation only. In addition to installation costs, some vehicle disabling systems (especially remote monitoring systems) may also require a monthly fee for maintenance and monitoring.

4.3.4 Who offers vehicle immobilization systems?

As illustrated in **Figure 4.3.b**, the market for VIS products and services is well served by a number of vendors.

Figure 4.3.b Vehicle immobilization system vendors

<p>AirIQ, Inc. Product: OnBoard™ 1099 Kingston Road, Suite 233 Pickering, ON, Canada L1V 1B5 Phone: 905-831-6444 Toll Free: 888-606-6444 http://www.airiq.com</p>	<p>GPS Management Systems Product: Asset Tracking 480 E. Northfield Drive, Suite 500 Brownsburg, IN 46112 Phone: 800-914-8247 Fax: 317-852-0742 http://www.gpsmanagement.com</p>	<p>Magtec Products (USA), Inc. Product: M5K 871 Coronado Center Drive, #200 Henderson, NV 89052 Phone: 888-624-8320 E-mail: info@magtecproducts.com http://www.magtecproducts.com</p>
---	--	---

¹⁴ The sections is taken from the overview of vehicle disabling systems on the Federal Motor Carrier Safety Administration Website: <http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/vehicle-disabling.htm>

QUALCOMM Incorporated Product: Vehicle Command & Control 5775 Morehouse Drive San Diego, CA 92121-1714 Phone: 858-587-1121 http://www.qualcomm.com	Safefreight Technology (USA), Inc. Product: SmartFleet™ 8000 N.E. Parkway Drive, Suite 200 Vancouver, WA 98662 Phone: 360-944-6722 Fax: 360-253-6424 http://www.safefreight.com	Satellite Security Systems, Inc. (S3) Product: GlobalGuard 6779 Mesa Ridge Road, Suite 100 San Diego, CA 92121 Phone: 858-638-9700 http://www.satsecurity.com
--	---	--

The VIT products of three of the vendors are highlighted below.

Safefreight Technology (ST)

The ST vehicle immobilization technology consists of an onboard “box” that can receive input from 8-12 sensors (analog or digital signals) and that can also be tied to the vehicle’s data bus, a GPS device, and a communications system that can use cell or satellite networks (Safefreight Technology, 2007). This is a web-based system that requires no software interface. Customers can choose between cell and satellite, or have both; in which case, an algorithm selects the one that is most cost-effective, thus ensuring almost 100% coverage at a minimum cost.

Customers may choose which types of sensors they want onboard (temperature, light, tank fill volume, etc.) that will function in conjunction with their device. ST consults with their customers to create response protocols that meet their customer’s needs and that can be modified at a later time, if necessary. When the Response Center receives the “real-time” notification of a sensor violation, ST security specialists immediately implement the associated response protocol, which includes contacting key personnel and/or the authorities as identified by the client, in the order specified by the client. These protocols and systems are predetermined so that key personnel can be reached at their office, at home or on the road, or through a 24/7/365 call center. In addition to events triggered from onboard sensors, ST also provides geo-fencing and landmark mapping capabilities. ST has the ability to provide remote ignition lockout and driver authentication.

Other ST technologies include a version of their device that can function in a battery mode on an untethered trailer, and can be configured to get power from the tractor when mated. A portable version of the onboard “box,” which operates on rechargeable batteries, has no external wires or antennas and does not require “line-of-sight” for GPS fixes. It can interface with wireless sensors onboard the tractor-trailer and has the ability to link to an electronic cargo manifest.

ST has over 1,000 units deployed in the United States and 1,500 in Canada. The vast majority of the units sold to date have been installed by the customer; ST provides installation instructions, a manual, and customer support. The cost of a base unit is \$625-\$700, plus \$35 to \$40/month/vehicle for reporting at a 2-minute interval. The cost of the dual reporting system adds \$350 for a modem plus a “Sim card,” and requires an additional service contract.

MAGTEC Products, Inc.

The MAGTEC® VIT technology provides various features and capabilities, including a driver authentication system, vehicle protection logic, hijack code, maintenance code, and an acceleration control system, among other features (MAGTEC, 2005). The MAGTEC Authentication System includes a keypad used by the driver to enter a pre-assigned PIN or a driver authentication code; without a correct code, the onboard eVID would not allow the truck to be started. The Protection Logic component is an automated vehicle disabling technology that allows the driver to leave the truck idling and will prevent any unauthorized person from driving that truck. The system also offers a hijack code or under-duress code, which once entered and after some predefined period of time, will send a distress message to the dispatcher. However, regardless of any communication system, the hijack feature will always work and disable/shutdown the vehicle; that is, once the hijack feature is activated by the driver, the vehicle will shutdown. The maintenance code feature allows the dispatcher to generate a one-time maintenance access code that can be used for a preset period of time (up to 99 hrs). If the truck is in maintenance mode and someone attempts to steal the vehicle, the truck will enter into a shutdown sequence after the maintenance period has expired.

Commercial vehicle immobilization systems are offered by a number of truck tracking vendors. Safefreight offers VIS as an add-on to its basic “smart truck” technology package. Cost \$700.

MAGTEC offers an integrated security package that includes a number of features including driver authentication and vehicle immobilization.

The Acceleration Control System™ (ACS) is the core of the MAGTEC VIT system. It is an eVID that restricts the acceleration capability of the vehicle, diminishing the maximum speed achievable by the vehicle by constant intervals triggered at predefined periods of time (see the Qualcomm section for more details about MAGTEC's ACS). These parameters, which define the shutdown process, are configurable over the air. This is a very important feature, particularly for FR5, which would allow the vehicle to be shut down quickly if so required (for example, in less than a mile, instead of shutting down gently over several miles). MAGTEC's remote deceleration technology has not, as of yet, been used in a real situation, but their idle protection technology (which ultimately uses the same VIT) has been used many times.

MAGTEC indicated that a customer could get a system that includes only the driver authentication portion of the technology without the disabling/shutdown technology. However, the VIT functionality portion of the technology is inherently part of the system and would be wired but not active. The VIT functionality could, in theory, be activated (if the vehicle has communication capabilities) even if the customer has not chosen to use that technology.

Other features include geo-fencing capabilities (for those vehicles equipped with GPS and communication systems), back office software and communication technologies for customers that do not want to go with complete packages (such as the one offered by Qualcomm), and, shortly, the availability of technology that will protect the trailer/cargo (at the present time, only the tractor is protected).

GlenHugh Enterprise (GHE)

GHE provides a modular platform consisting of different modules that cover different FRs. Specifically, the GHE platform consists of four separate modules that provide different levels of protection and can be configured to any communications carrier.

Module 1 (573): The 573 PPI (Passive Proximity Immobilizer), with driver authentication, is the primary immobilization system that ensures that a truck cannot be started and driven by an unauthorized operator. Disabling up to three vital circuits of the vehicle, the 583 system will not allow an unauthorized driver to start and drive the vehicle. GHE makes available authentication codes for lost codes via toll-free and fleet identification. The 573 PPI is an Underwriters Laboratory of Canada certified device.

Module 2 (898): The 898 Safe-Stop Immobilizer, with driver authentication, allows the truck to idle with the key removed. If a thief attempts to steal the vehicle while it is idling, As soon as the brakes are disengaged, any change in the engine revolutions triggers an engine shutdown. This device is being used by many trucking companies and public service fleets.

Module 3 (211): For FRs 1, 3, and 4, GHE's anti-hijack technology is adaptive and can be customized to any specific fleet requirement triggered by various initiating events such as pressing a button or opening the driver's door, the latter being a main feature for the company's anti-hijack technology. The primary goal is focused on safely bringing the vehicle to a stationary position and to distance the driver from the hijacker as quickly as possible. The hijacker has to gain access to the truck cab and when the door or brake valve is opened, the shutdown sequence is automatically initiated. The driver then has the option to allow the vehicle to shutdown, cancel shutdown, or offer the hijacker access to an override button that will immediately send an alert signal to the dispatcher, indicating that an unauthorized driver has taken control of the vehicle. Once this is done, the dispatcher has the option to shutdown the vehicle. The shutdown sequence consists of slowly opening and closing the fuel line while the truck retains power. The truck comes to a slow, albeit jerky, stop as the vehicle runs out of fuel. The relay timing increases so that the moving vehicle's engine slows down until it stops. During this shutdown sequence, the truck lights are also flashing and the horn or siren is sounding loudly.

Module 4 (1r2): The 1r2 provides the dispatcher with the ability to prevent a vehicle equipped with this device from starting. This is achieved remotely via a message sent wirelessly to the vehicle. Once the message has been sent and the device is activated, the vehicle will not start and an alarm (buzzing sound) will be heard, indicating that the vehicle has been immobilized.

GlenHugh Enterprise products allows carriers to select the level of protection they want for their vehicles.

4.4 Singapore HazMat Transport Vehicle Tracking System

In July 2005, Singapore began operating its HazMat Transport Vehicle Tracking System (HTVTS), the world's first hazmat transportation security system. The HazMat Transport Vehicle Tracking System is operated by the **Singapore Civil Defence Force (SCDF)**, the government agency responsible for protecting the country from terrorist attacks.

Singapore's HTVTS provides the SCDF real-time tracking of hazmat trucks carrying high-hazard materials over Singapore's road system. Alerts from trucks straying out of authorized routes or traveling during unauthorized hours are immediately sent to SCDF enforcement personnel by the HTVTS. Beginning October 2007, hazmat trucks are automatically immobilized by the HTVTS if the trucks violate route requirements.

4.4.1 Why did Singapore build the HTVTS?

Singapore is one of the largest petrochemical hubs in the world. Over \$21 billion has been invested in Singapore's petrochemical facilities at Ayer Merbau, and the economic output from these facilities accounts for 4%-5% of Singapore's GDP.

The events of 9/11 were the catalyst for development of the HTVTS. Singapore has a landmass of only 300 square miles and a population of 4 million (dense urban development across the island). Disruptions in Singapore's hazmat supply chain due to terrorist action could be disastrous – both to the safety of Singaporeans and to Singapore's economy.

The CNN International© video (control/click on link below) provides an overview of Singapore's HTVTS.

http://www.astratagroup.com/external/astrata_on_cnn.wmv

4.4.2 Regulations drive technology deployment.

The Singapore Civil Defence Force established hazmat transportation regulations in conjunction with Singapore's National Environmental Agency (NEA). In Singapore, like the United States, hazardous waste is a subset of the larger hazardous materials universe and waste transportation is co-regulated by the SCDF and Singapore's environmental agency.

The FMCSA FOT study suggests that government action will be necessary to ensure timely and wide-scale smart truck technology deployment but was silent as to the nature of government action needed. In Singapore, the government is using its regulatory authority as the forcing mechanism for technology adoption – SCDF regulations require hazmat transporters to adopt "smart truck" technology. Without this regulatory "push", a comprehensive hazmat security program would not be possible.

Singapore's regulations require hazmat carriers to deploy "smart truck" technology and to report shipment information on a real-time basis. The HTVTS is the implementing tool for anti-terrorism regulations issued by SCDF that require: ¹⁵

1. fleet operators to obtain a transport license for trucks that haul hazardous materials;
2. hazmat drivers to obtain a Hazmat Transport Driver Permit;
3. fleet operators to install a GPS tracking device and special license plates on trucks hauling (or having the capacity to haul):

¹⁵ URL - Singapore Civil Defence Force - *Requirements on Road Transportation of Petroleum and Flammable Materials*
http://www.scdf.gov.sg/downloads/FS_Licensing/Circular_on_Requirements_of_Road_Transportation_of_Petroleum_&_Flammable_Materials.pdf



July 2005 – Singapore became the first country in the world to implement a hazmat tracking system to deter terrorist attacks.



Video of Singapore's HazMat Transport Vehicle Tracking System.

Regulations are the key driver for Singapore's hazmat tracking program.

The HTVTS is the implementing tool for Singapore's hazmat security regulations.

- a. more than 3 tons of petroleum or flammable materials,
 - b. more than 1 ton of liquefied ammonia, chlorine, hydrogen chloride, hydrogen fluoride and methyl chloride,
 - c. hydrogen in long tubes (tube trailers),
 - d. any amount of arsine, phosphine and phosgene gases; and
4. trucks hauling regulated hazmat loads to follow approved hazmat transportation routes during approved transportation hours.

All vehicles monitored under the HTVTS are deemed as always transporting materials in amounts above the regulatory triggers of 3 tons and 1 ton. These vehicles must adhere to approved routes and hours of transportation at all times. Failure to do so will result in a violation registered by the HTVTS.

In the event of any violation detected by the HTVTS, the SCDF duty officer will contact the company concerned (via the contact number given in the application for transport license). The company is required to immediately contact the driver on the road to take corrective actions and report back to the SCDF. In this regard, the company must ensure that they are able to remain in communications with the driver at any time that the vehicle is on the road.

If there is a geofence violation, the vehicle's horns and blinkers are automatically activated. The driver must then stop the vehicle safely by the side of the road, and contact the SCDF. If the vehicle does not stop, or the company confirms that they have lost control of the vehicle or is unable to contact the driver within 2 minutes, the incident is treated as a security violation.

In the event that the driver is detained by SPF or if the vehicle is found without the driver, SCDF will contact the driver's company, which must ensure that they drive or tow away the vehicle within 1 hour. The company also has to provide SCDF with information (name, NRIC, and vehicle number) on the company personnel who will take the vehicle. Both the licensee and the driver are subject to enforcement actions and penalties for violations.

4.4.3 What is the technology behind the HTVTS?

A small, but sophisticated, computer/GPS tracking device installed on a hazmat truck allows officials at the SCDF headquarters control room to monitor the truck's location and movement in real-time. Hazmat trucks are restricted to certain routes and are only allowed to travel on the roads during certain times.

The system will trigger an alert in the event of the following:

- tampering with the tracking device;
- unauthorized diversion from approved routes;
- unauthorized transportation during prohibited hours;
- unauthorized entry into restricted areas; or
- unauthorized disengagement of trailers.

The HTVTS also monitors vehicle speeds

About 500 domestic trucks and 150 foreign hazmat haulers are currently monitored by the HTVTS. The technology underlying the HTVTS is highly scalable – any size fleet can be tracked and monitored, over any size road system.

The HTVTS relies heavily on GIS functionality. The HTVTS system developer, Astrata Group Limited, used MapInfo™ as the GIS platform to build the HTVTS.¹⁶ A case study published by MapInfo may be found in **Appendix E**. Astrata also provided the on-board tracking devices used by the SCDF.

Hazmat trucks entering exclusionary zones (e.g. geo-zones) in Singapore are automatically disabled by the HazMat Transport Vehicle Tracking System.



The computer/GPS device used by the HTVTS is half the size of a cell phone.

The HTVTS can automatically immobilize an off-route truck.

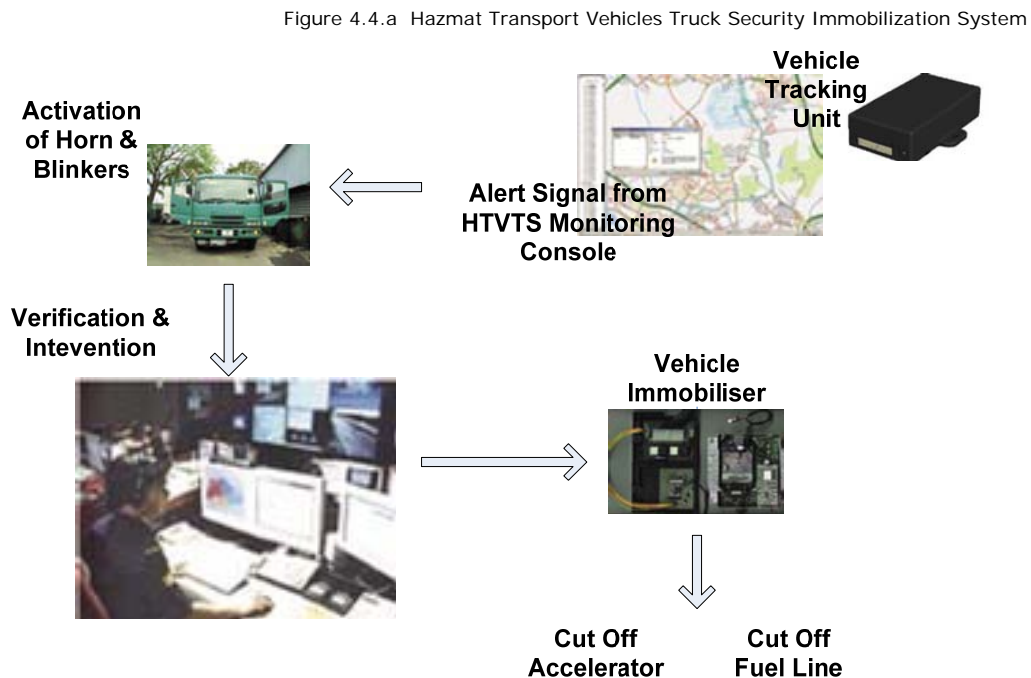
¹⁶ Astrata Group Ltd. Website: http://www.astratagroup.com/index.php?option=com_frontpage&Itemid=1

In October 2007, the SCDF activated immobilization functionality into the HTVTS. Vehicle immobilization is enabled by an add-on module to Astrata's tracking device. If a truck is off-route, the on-board device controls the truck's fuel injectors to prevent acceleration and limit throttle response. This will slow a vehicle progressively without interfering with its power steering and braking system. The vehicle is slowed safely to a low speed of 10km/hr to enable the driver to maneuver it to the side of the road before it comes to a full stop. For road safety considerations, the vehicle's horn and hazard warning lights will be activated before the immobilizer is triggered.

The SCDF phased in truck immobilization to give itself time to work through a number of issues. Examples of a few issues resolved by the SCDF include the following.

- What happens to a transponder when a truck is decommissioned?
- Does installation of a device void a truck's warranty?
- How can a truck be stopped without creating a road hazard?
- For old trucks using mechanical systems, how to install immobilization devices?

Figure 4.4.a illustrates how the HTVTS immobilization system works.



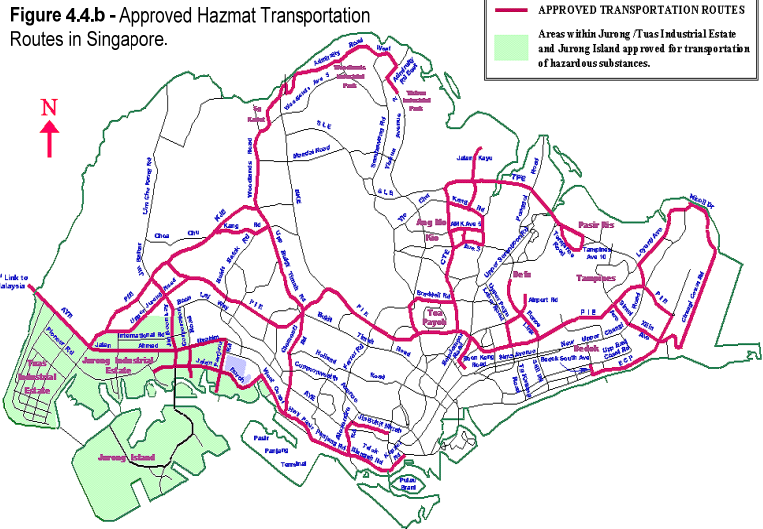
4.4.4 How does the SCDF factor risk assessment into its hazmat tracking program?

The SCDF established hazmat routes and hazmat restriction zones using a modified version of the U.S. Department of Transportation's hazmat routing criteria. DOT's hazmat routing criteria include: (1) cost (time, distance); (2) safety (accident prevention); (3) exposure – size of the population at risk; (4) emergency response capabilities; (5) burden on commerce; (6) congestion and transportation delays; and (7) property risk. In general, use of DOT hazmat routing criteria results in hazmat routes that avoid highly populated areas and areas of high commercial value. The SCDF supplemented DOT's hazmat routing criteria with criteria designed to enhance hazmat shipment security. Supplemental SCDF hazmat routing criteria include:

- socio-economic impact – potential cost of damage (direct and indirect);
- risk of hijack – factors/areas that make hijacking easier; and
- emergency response – rescue efficiency and police/military presence as a terrorist deterrent.

Singapore uses sophisticated GIS tools to establish hazmat routes & exclusion zones to maximize hazmat security.

Current hazmat routes in Singapore are illustrated in **Figure 4.4.b**. In general, the SCDF designed hazmat routes to prevent shipments from entering Singapore's Central Business District. The SCDF is continuing to refine hazmat routing and hazmat restriction zones using sophisticated geographic information system (GIS) tools to optimize hazmat route/restriction zone security.¹⁷



SCDF hazmat routing criteria are designed to prevent/mitigate use of hazmat shipments as weapons of mass destruction.

4.4.5 How does the HTVTS fit into Singapore's overall hazmat management program?

The project team also met with Mr. Jackson J.K. Lim of Singapore's Ministry of Home Affairs. Mr. Lim formerly served as a senior executive in the SCDF.¹⁸ The points below summarize some of the lessons learned by the SCDF in building and operating the HTVTS.

Organizational roles and responsibilities have to be clear.

Security cannot be too burdensome on industry.

A regulatory program will break down without a focused compliance & enforcement effort.

- **Voluntary doesn't work – regulations have to drive technology deployment.** The SCDF considered a voluntary call for installation of "smart truck" technology but concluded that it would be futile - a few good corporate citizens would deploy tracking systems and submit tracking data to the SCDF but that most companies would not. The SCDF also knew that incomplete or inconsistent deployment would defeat its hazmat security program. The SCDF decided that it had to use its regulatory authority to require companies to install tracking/immobilization devices and to report data.
- **The first and most important decision is what to regulate.** The decision on types of materials to regulate (and at what quantities) was the SCDF's most important decision when it designed its hazmat tracking program. This early-on decision determines how many companies will be regulated, the size and scope of the tracking program, etc.
- **Regulations and technology have to be in alignment.** A regulatory program that outreaches what is possible from a technology perspective will fail. The SCDF

¹⁷ Presentation Transportation Research Board conference 2004 - The National University of Singapore "Incorporating Security in HAZMAT Route Planning using GIS and AHP " provides an overview of Singapore's approach to using GIS to optimize hazmat security planning. [http://projects.battelle.org/trbhazmat/Presentations/TRB2004-BH.ppt#270,14,Assignment of Weights \(AHP\)](http://projects.battelle.org/trbhazmat/Presentations/TRB2004-BH.ppt#270,14,Assignment of Weights (AHP))

¹⁸ Michael Barclay (Coldstream Digital) and Dr. Sam Varnado (National Institute for Hometown Security) met with Mr. Lim in Boston on 3/31/2008. Mr. Lim is the Director of the Strategic Planning & Development Division of Singapore's Ministry of Home Affairs on 3/31/2008 in Boston. Singapore's SCDF is located in the Ministry of Home Affairs. Before assuming his current duties, Mr. Lim was a senior executive in the SCDF. He has detailed insight into the HTVTS and its development.

- carefully tailored “smart truck” technology to its regulatory needs for real-time vehicle tracking and vehicle immobilization.
- **Understand organizational roles and responsibilities – capture a clear mandate.** The SCDF was careful in crafting its regulatory and compliance programs to ensure that there was clarity in government roles and responsibilities. Also, the SCDF was careful to capture a clear and compelling mandate from Singapore’s legislative body to proceed.
- **Enhanced security cannot be too burdensome on industry.** The SCDF’s job is to protect Singapore from terrorists. But, the SCDF is also sensitive to the impact of enhanced security on Singaporean companies’ competitive position. The SCDF believes industry has to share in the cost of enhanced security but that the cost should be reasonable.
- **Carriers prefer not to be regulated, and will go to substantial lengths to avoid regulation (beat the system).** Some companies will resist regulation and/or will look for regulatory loopholes to escape being regulated. For example, shortly after the SCDF set a regulatory trigger of 3 tons of petroleum products, many carriers began using trucks with a fuel capacity lower than 3 tons. The SCDF is considering lowering the trigger to 2 tons. The SCDF has a robust compliance program to ensure high compliance by hazmat carriers. According to the SCDF, a weak compliance program will be quickly exploited.
- **An effective security program must include vehicle immobilization.** The SCDF believes that vehicle immobilization is a critical component of a hazmat truck security program. Just knowing where a truck is may not be enough. For example, even if the system detects a hijacking in progress, a terrorist can take the shipment into a vulnerable area and use it as a WMD unless there is a way to immobilize the truck.
- **Back-office systems are critical – require suitable investment.** The systems that ensure the smooth functioning of the administrative aspects of a truck tracking program are essential to success. Administrative systems include financial management (fee processing), registration, help desk, and user rights/access management.
- **People have to be involved in decision-making – the system cannot do it all.** It is possible to automate most of the decision-making in a truck tracking system. However, the system cannot manage every situation especially those where communications with regulated parties or response agencies is important.
- **Things will go “haywire” – build in contingencies.** Even the best designed systems will go “haywire”. It is important to invest in contingencies to minimize the impact of problems.
- **Driver identification is important.** The SCDF did not require biometric devices on trucks to prevent unauthorized drivers from gaining access to a hazmat shipment. The SCDF decided that biometric devices cost too much and would be disruptive given that trucks often have multiple drivers. The SCDF believes, however, that there needs to be an administrative/regulatory framework to screen out people that should not be handling hazmat shipments.
- **Public outreach is critical.** It is important to have a good public communications plan – especially a plan to work with industry as new requirements are put into place. Building a good system is important, but it’s also important to build public

The SCDF believes vehicle immobilization is a critical component of a hazmat security program.

Investment in backend administrative systems is critical.

Automate business processes to the extent possible, but recognize the need for human involvement.

Things will go “haywire”. Invest in contingencies.

The SCDF does not believe biometrics are feasible but believes it is important to prevent “bad” drivers from accepting hazmat loads.

Public outreach is critical to making the program work.

outreach and pilot programs that help companies come into compliance with regulatory requirements.

4.5 U.S. Transportation Security Administration - Hazmat Truck Security Pilot

After the FMCSA finished its Hazmat Safety and Security Technology Field Operational Test in November 2004, Congress directed the **U.S. Transportation Security Administration's** (TSA) to undertake the TSA Hazmat Truck Security Pilot (HTSP) project. The purpose of the pilot project was to demonstrate that a hazmat truck tracking center was feasible from a technology and systems perspective and to determine if existing commercial truck tracking systems can interface with government intelligence centers and first responders.



Congress directed TSA to undertake the Hazmat Truck Security Pilot project. TSA demonstrated that a truck

The contract for the Hazmat Truck Security Pilot program was awarded to General Dynamics Advanced Information Systems (GDAIS) of Buffalo, NY in October 2005. Work under the contract was completed April 2008. The contract had three tasks.

1. Develop and demonstrate a prototype for a centralized truck tracking center that could be used to continually track truck locations and load types. The truck tracking center would also be used to coordinate incident response with a government intelligence operations center, state, local, and Federal law enforcement agencies and first responders.
2. Develop and demonstrate a non-proprietary universal interface or set of communication protocols that would allow alerts and tracking information to be transmitted from all commercially available tracking systems to a prototype truck tracking center.
3. Analyze the feasibility and benefits of applying a risk-based approach to identifying and managing hazmat security risks and incidents involving trucks on U.S. highways; demonstrate the capability of using the Hazmat Truck Security System (HTSS), with a commercial-off-the-shelf (COTS) rules-based risk assessment tool; and conduct a public showcase demonstration of the entire HTSS.

The Hazmat Truck Security Pilot (HTSP) program demonstrated that a truck tracking system is feasible from a technology and systems perspective.

4.5.1 What are the building blocks of a hazmat truck tracking center?

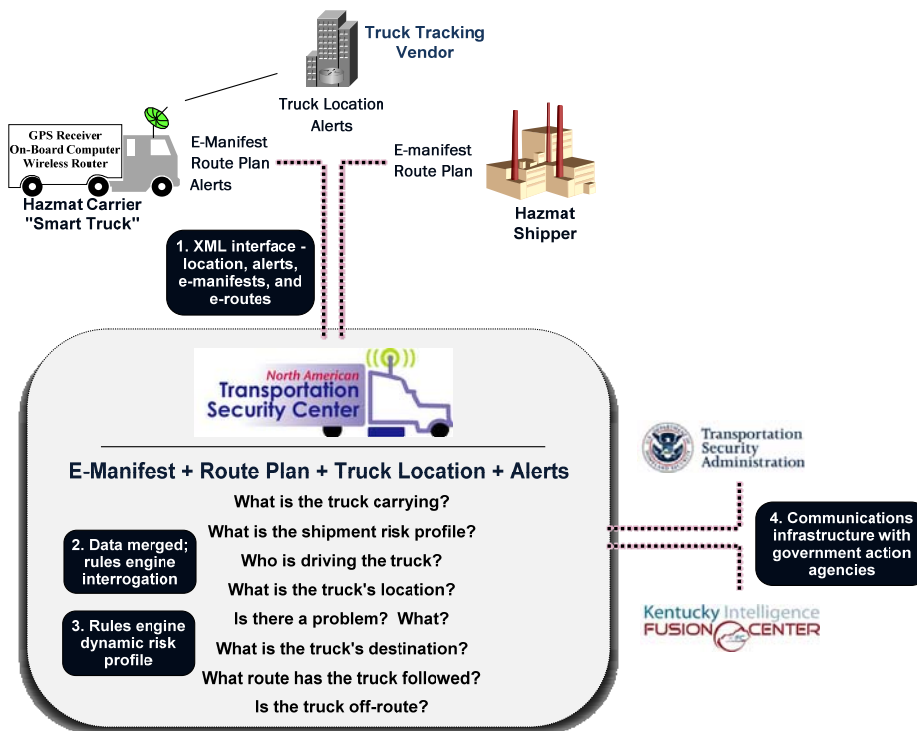
Figure 4.5.a presents a general schematic of a hazmat truck tracking center. As indicated in Figure 4.5.a, four basic functional components – or building blocks - are needed to build a hazmat truck tracking system.

1. An **XML-based interface** with shippers, carriers, and truck tracking vendors feeds data to a hazmat truck tracking center.
2. A hazmat truck tracking operations center **merges data** flowing into it to create actionable information for government agencies.
3. A **risk engine** provides dynamic risk profiling of hazmat shipments between gate-out and gate-in to identify shipments that present true risk.
4. A **communications infrastructure** supports efficient interaction/consultation with government action agencies.

4.5.2 Shippers, carriers, and truck tracking vendors have to deploy “smart truck” technology and submit data to enable a truck tracking center.

A hazmat truck tracking center is dependent on data flow from shippers, carriers and truck tracking vendors. Data is the raw product that a truck tracking center converts into actionable intelligence. Efficient and timely processing of data gives the center the

Figure 4.5.a Building blocks of a hazmat truck tracking center.



The building blocks of a hazmat truck tracking center are:

1. an XML –based communications interface;
2. an operations center that processes data into actionable intelligence;
3. a business rules engine for dynamic risk profiling of hazmat shipments; and
4. a communications infrastructure for collaboration with action agencies.

ability to answer the questions presented in Figure 4.5.a and allows it to effectively support government action agencies when a transportation security incident is declared.

However, a truck tracking center will fail unless smart truck technology is widely deployed and shippers, carriers and truck tracking vendors submit data to the truck tracking center. Currently, there is no regulatory requirement that hazmat shippers deploy smart truck technology or submit data to a truck tracking center.¹⁹

Industry groups have advocated voluntary measures for hazmat technology deployment and data reporting. However, voluntary industry measures – while conceptually appealing – rarely work. The FMCSA FOT study (refer to Section 4.1) acknowledged the problem of industry-led voluntary programs by suggesting that “government intervention” (e.g. regulations) will be needed to stimulate smart truck technology deployment and data reporting. This argument for “government intervention” is buttressed by DHS’s recent experience in its efforts to beef up security at chemical production plants in urban areas. In that case, an industry-led voluntary initiative to upgrade chemical plant security resulted in such a tepid industry response that DHS had to take the program back and issue regulations to require chemical companies to institute security programs (refer to Section 2.2.4).

4.5.3 The HTSP prototype design reflected assumptions about technology deployment and data reporting.

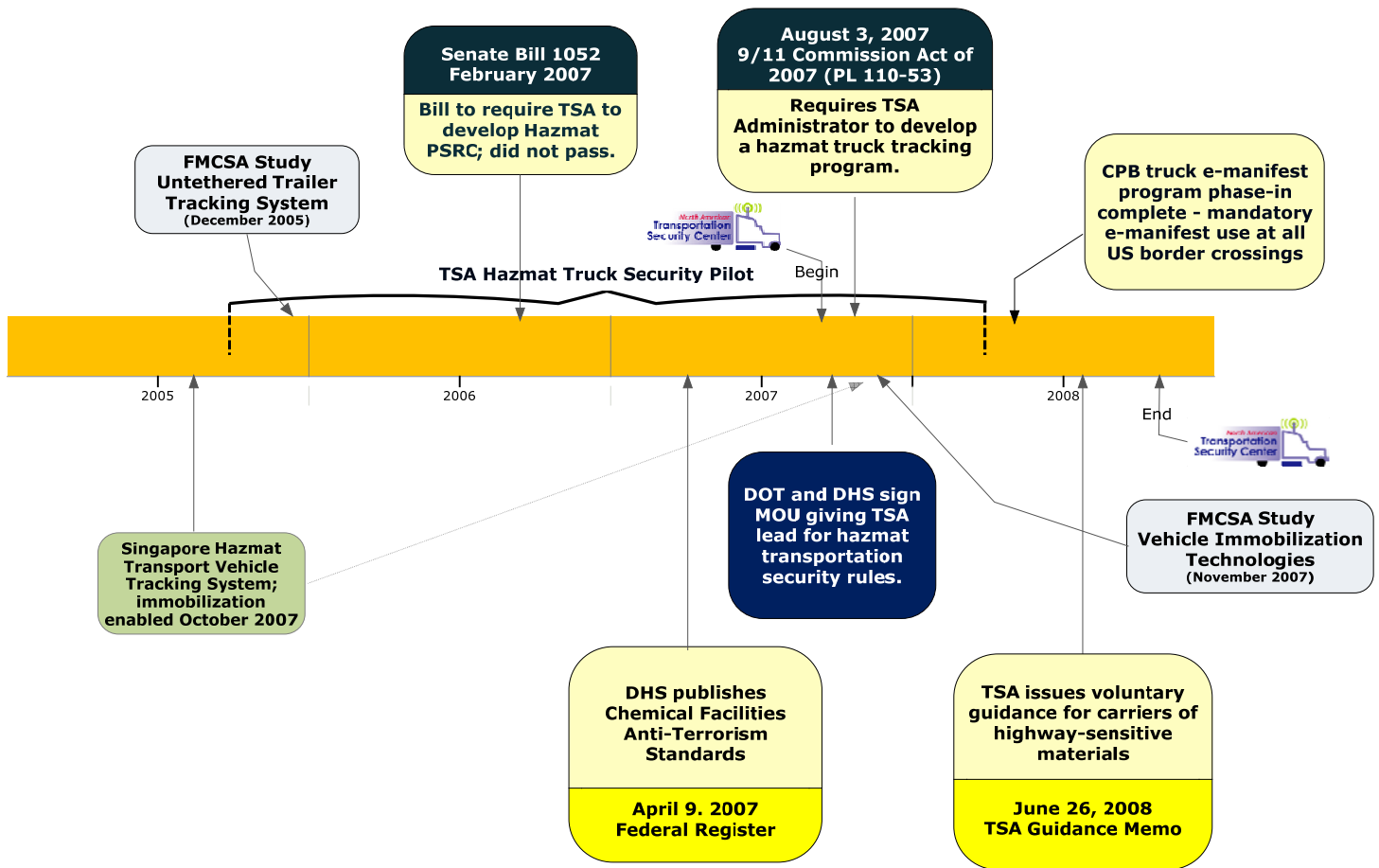
Figure 4.5.b shows the timeline of events surrounding the HTSP project. The HTSP project began in October 2005 and ended April 2008. The FMCSA’s seminal Field Operations Test was completed a year before the HTSP project began. While the FOT project report suggested that regulations should drive

To succeed, a hazmat truck tracking center needs data. Hazmat carriers have to deploy smart truck technology, and shippers, carriers, and truck tracking vendors must submit

It is unlikely that hazmat trading partners will voluntarily submit data to a truck tracking center.

¹⁹ The exceptions are munitions and radioactive material shipments. However, these shipments represent only a small fraction of the total number of high-risk hazmat shipments in the U.S. Refer to Section 2.4.2.

Figure 4.5.b The HTSP project began October 2005 and ended April 2008.



In late 2005 when the HTSP began, there was uncertainty about technology and regulatory issues.

technology deployment and data reporting – especially in light of positive ROI generated by smart truck technology – the time was not right in late 2005 for a regulatory push by federal agencies (refer to Section 4.1). The responsibility for regulation of hazmat shipments was in transition from DOT to DHS, and a number of thorny technical and regulatory uncertainties existed. The results of the FMCSA field tests on vehicle immobilization systems (see Section 4.3) and untethered trailer tracking systems (see Section 4.2) were not yet available, and the concept of operations for a hazmat truck tracking center had been only mildly developed in the FOT. Moreover, there was a great deal of uncertainty about the role that regulations would play in securing the nation’s hazmat supply chain.

The HTSP project was hugely successful in that it proved that a hazmat truck tracking center is feasible from a technology perspective.

Even though the HTSP prototype’s functionality was limited by industry participation, the HTSP pilot was highly successful. It proved that a hazmat truck tracking center is technically feasible and that smart truck technology can be crafted into an effective and efficient system for tracking hazmat shipments. However, the pilot fell far short of advancing a regulatory and implementation framework that would allow TSA to move forward with its hazmat truck tracking program. This is not a criticism of the HTSP pilot or the work done on it – development of a framework for implementing TSA’s hazmat truck tracking program was not part of the mission of the project team.

4.6 U.S. Customs and Border Protection – ACE Truck E-Manifest

The **U.S. Customs and Border Protection** (CBP), an agency of the U.S. Department of Homeland Security, is responsible for protecting the nation's borders and for promoting the free flow of legitimate goods into the country. In early 2001, CBP began a large, multi-year effort to rebuild and modernize its information systems. CBP's Automated Commercial Environment (ACE) – CBP's new information system - will arm CBP personnel with the tools and information they need to decide which incoming shipments should be targeted for inspection at the border. ACE will also automate time-consuming and labor-intensive transactions so that legitimate shipments can move through ports and border crossing quickly and efficiently.



The U.S. Customs and Border Protection's Automated Commercial Environment (ACE) enhances border security and speeds the flow of commercial traffic into the U.S.

In 2002, Section 343(a) of the Trade Act of 2002 (PL 107-210) required CPB to:

"promulgate regulations providing for the transmission to the Customs Service, through an electronic data interchange system, of information pertaining to cargo destined for importation into the United States or exportation from the United States, prior to such importation or exportation."

CBP issued regulations under 19 CFR Section 123.92 that requires all trucks crossing customs from Canada destined to the U.S.A. with freight on board to submit an electronic truck manifest to CBP before arriving at the border.²⁰ If a truck arrives at customs without submitting a Manifest electronically, it will be refused access into the United States. A truck returning to the United States empty or entering Canada from the United States is not required to submit an E-Manifest.

The ACE truck e-manifest will help create a secure and streamlined environment for processing and releasing cargo at the land borders. It was launched in conjunction with the deployment of the CPB's ACE Secure Data Portal, which will bring enhanced security and commercial account capabilities to all land border ports across the nation. Carriers can use the ACE Secure Data Portal or commercial Electronic Data Interchange (EDI) systems to create an e-manifest and submit it along with mandatory advance cargo information to CBP in advance of a shipment. This allows CPB to pre-screen the crew, conveyance, equipment, and shipment information before the truck arrives at the border. E-manifests allow CBP officers focus their efforts and inspections on high-risk commerce, minimizing unnecessary delays for legitimate, low-risk commerce.

4.6.1 E-manifests and RFID systems speed trucks past CBP inspection stations.

The ACE e-manifest capability consolidates previously separate cargo release systems into a single, integrated computer interface for CBP officers and allows truck carriers to prepare and submit electronic truck manifests prior to arrival at a land border port of entry. With advance access to truck cargo information, CBP officers are able to pre-screen trucks and shipments, and dedicate more time to inspecting suspicious cargo without delaying the border crossings of legitimate carriers. E-manifests are also more efficient with an average processing time that is 33 percent faster than a traditional paper manifest.

The ACE truck e-manifest system uses electronic manifests and RFID to speed truckers through border inspection posts.

Since November 2007 when ports in Alaska went on-line, e-manifest use has been mandatory at all 99 U.S. land border ports.

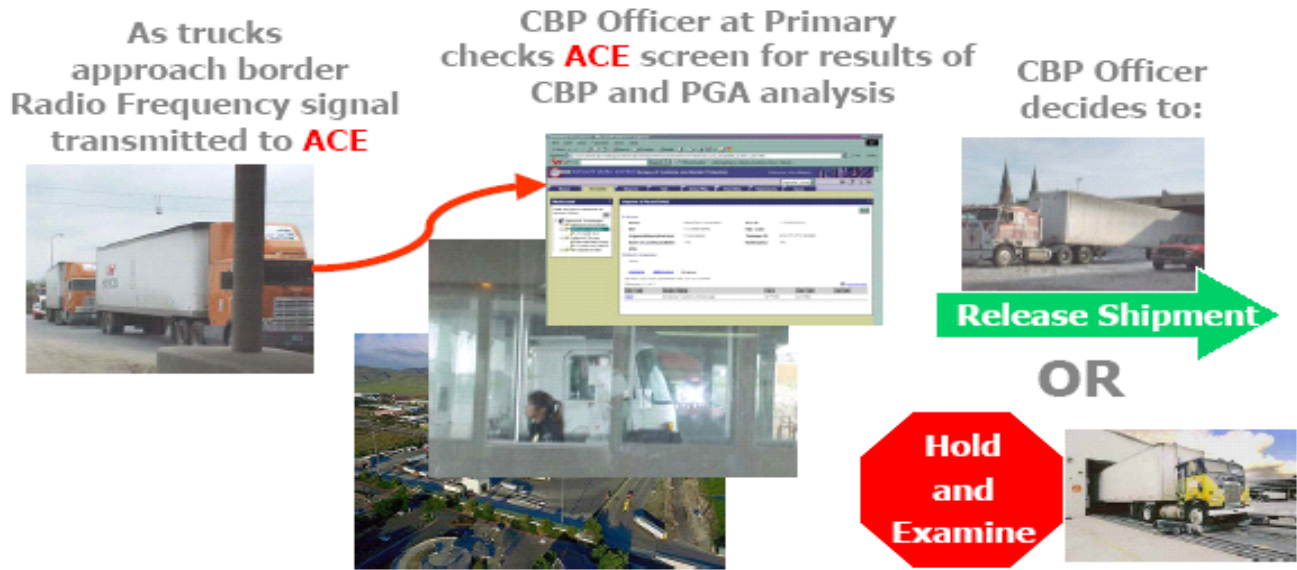
As illustrated in **Figure 4.6.a**, when a truck approaches the border crossing, the e-Manifest is automatically retrieved along with the matching pre-filed entries, in-bond requests, and other release declarations for the CBP Officer to view and process. The e-manifest must be transmitted at least one hour prior to the carrier's arrival at the

²⁰ Truck e-manifest Federal Register notices are listed below.

- Modification to data elements required for participation in the truck e-manifest program - 70 FR 13514, March 21, 2005
- Ability of truck carriers to use third parties to submit manifest information in the ACE test - 71 FR 15756, March 29, 2006
- Ability of third parties to submit manifest information on behalf of truck carriers via the ACE secure data portal – 72 FR 50, March 15, 2007

border. The CBP Officer can either release the truck, or hold the truck for further processing.

Figure 4.6.a. ACE Truck E-Manifest.



Receiving the electronic manifest information early allows CBP and other border security agencies to pre-screen the manifest through multiple checks before the truck arrives at the port. The receipt of e-Manifests enables CBP Officers to focus their efforts and inspections on high-risk commerce, thereby minimizing unnecessary delays for legitimate, low-risk commerce.

From the Carrier's perspective, a huge benefit of ACE is that Carriers no longer have to pay import duties and fees on a transaction-by-transaction basis. Beginning June 2004, Carriers are issued a monthly statement by CBP and can make one monthly payment for all transactions. This changes a business practice begun by Customs in 1789 in which customs duties and fees were processed one entry at a time.

The ACE truck e-manifest system offers highway carriers the ability to move goods across the border faster and more efficiently. In addition to expedited trade flows, **Figure 4.6.b** lists benefits that ACE truck e-manifest offers the government and the trade community.

Figure 4.6.b. ACE Truck E-Manifest Benefits

Enhanced border protection	<ul style="list-style-type: none"> • Availability of pre-arrival information • Cargo tracking; access to more accurate and timely transaction information • Multi-agency enforcement collaboration
Enhanced efficiency and lower costs	<ul style="list-style-type: none"> • Promote information sharing among federal, state, and local governments • Accelerate border clearance • Eliminate paper systems
Trade facilitation	<ul style="list-style-type: none"> • Single-window transaction filing for the trade community • Harmonization of government data requirements • Online access to data • Improved visibility of conveyance and cargo status

The ACE truck e-manifest system saves carriers money and expedites the flow of trade across the border.

4.6.2 Carriers can use CBP's portal to submit a truck e-manifest; CBP's e-manifest has 70 data elements.

The ACE truck e-manifest creates a secure and streamlined environment for processing and releasing cargo at the land borders.

Carriers are able to file an e-Manifest through the ACE Secure Data Portal or by utilizing the services of a U.S. Customs and Border Protection (CBP) tested solution provider. Carriers may opt to use another party to file the trucking e-Manifest on their behalf, such as Customs brokers, border processing centers, or other carriers. Truck carriers without an ACE portal account may use a third party with an ACE portal account to electronically transmit truck manifest information via the ACE portal on their behalf.

The ACE **truck e-manifest** has 70 data elements.

A step-by-step guide for creating and submitting an electronic manifest has been prepared by CBP.

http://www.cbp.gov/xp/cgov/trade/automated/modernization/carrier_info/electronic_truck_manifest_info/

There are two ways an e-manifest can be submitted to CBP.

1. The ACE Secure Data Portal provides a web-based method to submit data to CBP. The portal is readily accessible on the Internet and is free to all users. Portal users key data in manually and then submit information directly to CBP.
2. Electronic data interchange (EDI) is an electronic transmission of data directly from one computer system to another. Information sent to ACE via EDI will be validated and processed. E-manifests can be sent to ACE either by the carrier or by a third party service bureau. Carriers have three options for using CBP-tested EDI software.
 - Self-developed EDI interface – A carrier develops in-house software that is tested by CBP and interfaces with ACE.
 - Software application provided by a software vendor – A carrier utilizes software provided by a vendor that has been tested by CBP. Often, these software applications enable carriers to pull the data required to populate the eManifest from the software they use in their daily business practices.
 - Service provider – A carrier employs a third party to enter and/or transmit manifest data on his or her behalf. This third party is using software that has been tested by CBP.

Carriers can prepare and submit e-manifests on CBP secure portal or let others submit e-manifests on their behalf.

In the ACE Secure Data Portal, truck carrier accounts are organized by Standard Carrier Alpha Codes (SCACs). There are five sets of master data that can be stored in the truck carrier's ACE account. Storing these items will reduce the time it takes to create a manifest. This information may be stored in an account for future retrieval, or they can be entered each time a manifest is prepared. These sets of master data are as follows:

Carriers with accounts on CBP's portal can keep their shipping data on file to make e-manifest preparation fast and easy.

1. Drivers/Crew
2. Conveyance (power units)
3. Equipment (trailers, containers, chassis etc.)
4. Shipper (names and addresses)
5. Consignee (names and addresses)

CBP lists the following benefits of preparing and submitting e-manifests via its secure portal.

- Easy-to-use, simple screens, including a unique auto-complete feature on forms, allows anyone to step in and complete a manifest quickly and efficiently;
- Straightforward dashboard screen, updated in real-time, giving an at-a-glance view of all shipments and their status;
- Powerful search and filter features, to quickly and easily locate a manifest;
- Easy-to-read data entry screens for shipment information;

- Automatic shipment status notifications sent via e-mail to trade chain partners;
- Create and print all the forms and reports to clear Customs, including the ACE cover sheet;
- Complete submission history of all shipment and reporting activity for tracking and compliance auditing.

Another advantage of ACE is that ACE participants do not have to pay duties and other fees on a transaction-by-transaction basis. Through the Periodic Monthly Statement, they can make a consolidated payment to Customs on a monthly basis, streamlining accounting and report processing.

The truck e-manifest has 70 data elements. Data elements (1) – (12) listed below are the core data elements for the truck e-manifest. Data elements (13) – (70) are included on the e-manifest as applicable. Those that are relevant to hazmat shipments are also listed below.

(1) Conveyance number, and (if applicable) equipment number (the number of the conveyance is its Vehicle Identification Number (VIN) or its license plate number and State of issuance; the equipment number, if applicable, refers to the identification number of any trailing equipment or container attached to the power unit. For purposes of this test, both the VIN and the license plate number are required);

(2) Carrier identification (i.e., the truck carrier identification SCAC code (the unique Standard Carrier Alpha Code) assigned for each carrier by the National Motor Freight Traffic Association);

(3) Trip number and, if applicable, the transportation reference number for each shipment (The transportation reference number is the freight bill number, or Pro Number, if such a number has been generated by the carrier.);

(4) Container number(s) (for any containerized shipment, if different from the equipment number), and the seal numbers for all seals affixed to the equipment or container(s);

(5) The foreign location where the truck carrier takes possession of the cargo destined for the U.S.;

(6) The scheduled date and time of arrival of the truck at the first port of entry in the U.S.;

(7) The numbers and quantities for the cargo laden aboard the truck as contained in the bill(s) of lading (this means the quantity of the lowest external packaging unit);

(8) The weight of the cargo, or, for a sealed container, the shipper's declared weight of the cargo;

(9) A precise description of the cargo and/or the Harmonized Tariff Schedule (HTS) numbers to the 6-digit level under which the cargo will be classified.

(10) Internationally recognized hazardous material code when such cargo is being shipped by truck;

(11) The shipper's complete name and address, or identification number.

(12) The complete name and address of the consignee, or identification number.

(13) DOT number;

(14) Person on arriving conveyance who is in charge;

(15) Names of all crew members;

(16) Date of birth of each crew member;

(17) Commercial driver's license (CDL)/drivers license number for each crew member;

(18) CDL/driver's license State/province of issuance for each crew member;

(31) Hazmat endorsement for each crew member;

(42) Conveyance insurance company name;

(43) Conveyance insurance policy number;

(44) Year of issuance;

(45) Insurance amount.

CBP requires the submission of a extensive data on each in-coming shipment of goods.

Some of CBP's e-manifest data elements are specific to hazmat shipments (see yellow highlighted items).

(65) Hazmat contact:

4.7 Ontario Ministry of the Environment – Hazardous Waste Information Network

On January 1, 2002, the **Ontario Ministry of the Environment (MOE)** issued new regulations for its hazardous waste program. The central feature of MOE's regulations was a requirement that hazardous waste generators would be obligated to pay a new set of fees. Ontario's fee objective was to capture about \$10 million/year in new regulatory fees.

The Hazardous Waste Information Network (HWIN) was the web-based system MOE built to support generator, hauler, and receiver registrations and to collect regulatory fees. HWIN had more to offer, however. It was also North America's first hazardous waste electronic manifest system. HWIN performed exceptionally well as a registration and fee collection system. However, only a small percentage of manifest transactions shifted from paper to electronic.

This section reviews MOE's experience and explores the reasons for low e-manifest adoption in Ontario.

4.7.1 What is Ontario's Regulation 347? Why was it enacted?

The Ontario Ministry of the Environment (MOE) is responsible for overseeing the hazardous waste program in the province. Regulation 347, Ontario's hazardous waste rule, is almost a mirror image of EPA's hazardous waste rule. Like EPA's rule, Regulation 347 includes a comprehensive manifest system to track hazardous wastes from the point of generation to final disposal. Regulation 347 differs from EPA rules in one major respect. It allows waste generators, transporters, and receivers to use e-manifests in lieu of paper manifests provided that they process their e-manifest transactions through the Hazardous Waste Information Network (HWIN), an on-line system managed by MOE. Ontario companies have had the option of using e-manifests in lieu of paper manifests since 2002.

There are about 8,000 hazardous waste generators and 200,000 hazardous waste shipments/year in Ontario. Since January 1, 2002, Regulation 347 has required hazardous wastes generators to visit the HWIN on-line registry once per year to update their corporate profiles and to pay an annual registration fee. The registration requirement applies to generators of hazardous waste in Ontario as well as out-of-province generators – including many U.S. companies – that ship waste to Ontario for treatment or disposal. In addition to the annual registration fee of Cad\$50, hazardous waste generators are also required to pay the following regulatory fees for waste shipments that originate or end in Ontario: 1). Cad\$5 for each manifest used to ship waste off-site; and 2). Cad\$10/ton of hazardous waste generated.

Ontario's regulatory fee provisions are not unusual. Many states in the U.S. – including Kentucky - have regulatory fee requirements on the books especially related to their hazardous waste programs. However, Ontario's requirements are notable in terms of the amount of revenue they generate. By design, MOE's Regulation 347 hazardous waste fees create a revenue stream of almost Cad\$9 million/year for the province. By the end of 2008, Ontario will have collected over Cad\$60 million under Regulation 347's hazardous waste regulatory fee program.

Even with MOE's hefty fee schedule, e-manifest usage has the potential to generate benefits of ~1.5x the cost of MOE's regulatory fees due to the inherent cost savings associated with e-manifests.²¹

²¹ B/C= US\$15million/CAD\$9million = US\$15million/US\$10= 1.5

B = 200,000 x \$75 = \$15 million potential annual e-manifest cost savings
(~200,000 manifest transactions/year in Ontario; EPA e-manifest unit cost savings = US\$75/manifest)

C = MOE regulatory fees of ~Cad\$9 million/year ~US\$10million.



Ontario's regulations are similar to EPA's regulations. Ontario has, however, allowed companies to use electronic manifests since 2002.

Ontario designed Regulation 347 to generate **Cad\$10 million per year in revenue for the province**. MOE has collected over Cad\$60 million in revenue from hazardous waste regulatory fees since 2002.



HWIN is the only hazardous waste e-manifest system in North America; serves as the **implementing tool** for Ontario's hazardous waste regulations.

HWIN was built around the regulatory needs of waste

4.7.2 What is the Hazardous Waste Information Network? How does it support Regulation 347? ²²

The Hazardous Waste Information Network (HWIN) is a web-based system that allows hazardous waste generators, transporters, and receivers to register their activities with MOE on-line, and to make payments for fees associated with Regulation 347. HWIN also enables users to create and process electronic manifests over the web making HWIN the first e-manifest system for hazardous wastes in North America.

HWIN was designed specifically to serve as the implementing tool for Regulation 347, allowing for the efficient integration of Regulation 347's fee collection requirements with the business processes associated with the manifesting of hazardous waste. The primary users of the HWIN system are hazardous waste generators, carriers, and receivers in Ontario. Generators, carriers and receivers outside Ontario with manifest transactions that originate or terminate in Ontario are also able to use HWIN.

4.7.3 Who are the system users? How do they use HWIN?

HWIN was built around the regulatory needs of waste generators that ship waste into or out of Ontario. There are, however, other system users. Other hazardous waste trading partners – waste haulers (transporters) and waste receivers (waste management firms) – also use HWIN. Within MOE, HWIN also meets a number of administrative and enforcement needs.

4.7.3.1.1 HWIN was built around the regulatory needs of waste generators.

Generators use HWIN to complete registration activities, including payment of annual registration fees, and to prepare and process electronic manifests. Generators also use HWIN to pay fees associated with manifest transactions. In addition, every generator has access to real-time data on their manifest transactions, and may use HWIN as an electronic repository for their manifest data. Carriers and receivers are not subject to fee requirements of Regulation 347 but may use HWIN to engage in electronic manifest transactions with waste generators and to gain access to their manifest transaction data.

Figure 4.7.a illustrates a screen shot of a typical "My HWIN" page owned by a fictional Ontario waste generator - Max Phillips of the Canadian Industrial Waste Company of Wama, Ontario

The list of wastes generated at Wama – including information on waste characteristics – may be found by clicking the 'registered wastes' tab. Max may add or delete wastes to the list any time. Before HWIN was implemented, companies had to file requests for waste list changes by paper with MOE. It took, on average, about three months for MOE to respond. Until the company had MOE's approval, it could not make the process change at the facility that would create the new waste product.

The 'open manifests' tab lists manifests that have been initiated at the Wama facility but that have not completed the complete manifest business cycle as well as information about those manifests (e.g. signed by generator/transporter, in transit, load diversion, load discrepancy, etc.). The 'closed manifest' tab lists manifests that have completed the full business cycle and detailed transactional data about those shipments.

HWIN allows users to manage all financial transactions associated with Regulation 347 (adding funds to an on-line account; regulatory fee payments). Note that HWIN computes and assesses fees (waste tonnage, manifest) for each transaction as it occurs. The 'account status' tab provides detailed information on financial transactions (payments made, dates, amounts, etc.).

Max can click on any manifest listed in column one, 'manifest number', and view a copy of the completed manifest (PDF for paper manifests or e-manifest w/digital signatures).

²² Hazardous Waste Information Network <http://www.hwin.ca/hwin/index.jsp>

Figure 4.7.a. My HWIN Page

hwin

MY HWIN

Canadian Industrial Waste Co.
1234 Garbage Lane, Wama, Ontario, Canada POS 1K1

Generator ID: ON1234567

'My HWIN' Page Owner & User Rights Authorization

User: Max Phillips
Rights: Administrator

[My HWIN](#) > [My HWIN Home](#)

HWIN NOTICES

01/06/02: You need to enter a password combination to use when you sign on to HWIN. Your password combination will be different from the user name/password combination you use to sign in to HWIN. [Click here](#) to get your electronic signature PIN/password.

Company Information

System Wide Notices From HWIN

[Build eManifest](#)

Link to Build eManifest

List of manifests which have not completed the complete business cycle.

PAYMENTS PENDING		OPEN MANIFESTS			REGISTERED WASTES		ACCOUNT STATUS		CLOSED MANIFESTS	
Number of manifests with payments pending: 10					Total amount due: \$308.00		Pay All			
Manifest No.	Type	Carrier	Receiver	Date Shipped	Amount Due	Payment				
98001078	Paper	1234-5VWXYZ	987-65A432	09/08/02	\$15.00	Pay This Manifest				
98001079	Paper	1234-5VWXYZ	987-65A432	19/06/02	\$11.00	Pay This Manifest				
98001080	Paper	1234-5VWXYZ	987-65A432	26/06/02	\$31.00	Pay This Manifest				
98001081	Paper	1234-5VWXYZ	987-65A432	27/05/02	\$15.00	Pay This Manifest				
98001082	Paper	1234-5VWXYZ	987-65A432	05/05/02	\$90.00	Pay This Manifest				
98001033	Electronic	1234-5VWXYZ	987-65A432	12/04/02	0.00	Pay This Manifest				
98001032	Electronic	1234-5VWXYZ	987-65A432	01/04/02	0.00	Pay This Manifest				
98001028	Paper	1234-5VWXYZ	987-65A432	03/03/02	0.00	Pay This Manifest				
98001021	Paper	1234-5VWXYZ	987-65A432	20/03/02	\$15.00	Pay This Manifest				
98001019	Paper	1234-5VWXYZ	987-65A432	15/03/02	\$10.00	Pay This Manifest				
98001014	Paper	1234-5VWXYZ	987-65A432	30/01/02	\$21.00	Pay This Manifest				
Add to Prepaid Account						View All				

List of manifest transactions for which payment is due; provides payment mechanism.

Transaction Type

Carrier, Receiver & Shipment Date

Manifest number; click to view manifest form and detailed information on the transaction

List of wastes generated at the facility; waste stream profiles.

Regulatory fees due for transaction: waste tonnage and manifest transaction fee

Payment mechanism; pay total due or by transaction.

HWIN Capabilities and Features

- Registration forms are pre-filled with data from MOE data sources to make the registration process faster and to validate MOE-held data. On-screen e-manifest wizards include data checks and validations to prevent generators from making errors as they prepare e-manifests
- User rights are established and managed by company administrators (i.e. Max has administrator status for his company). User rights are established at the individual level. Each user manages his/her secret PIN/passwords to the HWIN system.
- As parties to the e-manifest transaction sign the e-manifest, their portion of the form is "locked" so that other parties cannot change the form later. As each e-manifest transaction takes place (ie waste shipment chain-of-custody change), a 'snapshot' of the e-manifest form is taken and stored in the HWIN database. E-manifest forms/transactions are programmed to follow the business process workflow. For example, a load rejection by a receiving facility initiates a set of business processes that change the routing of the e-manifest form. Workflow events trigger notifications and on-line approvals and help connect generator, transporter and receiver waste manifest business processes. E-mail is the communication mechanism for alerts.
- A generator may only use transporters/receiving facilities that MOE has authorized (permitted) to transport or manage the generator's specific waste type. HWIN business rules are applied as the generator prepares the e-manifest to prevent a transporter/receiver mismatch with a generator's waste stream.
- HWIN allows a generator to search for vendors (transporter, receiver) that may manage the type of waste the generator produces and to build/maintain a list of preferred vendors.
- HWIN replaces record retention requirements for generators, transporters and receivers (for e-manifest transactions only). HWIN provides system users 24/7 access to account and transactional data. Users manage their corporate data – profiles, user rights, company information, etc. – directly in HWIN providing MOE with high quality, up to date data about system users.
- HWIN allows generators, transporters and receivers to sign e-manifests by telephone. Using their PIN/passwords, the parties can interact with the HWIN database to apply an electronic signature to a manifest. HWIN allows MOE inspectors - using a cell/PDA - to type in a waste transporter's license plate number to retrieve the hauler's e-manifest(s).

The My HWIN page lets a generator view and change waste profiles, make payments, view open and closed manifest

4.7.3.2 Waste transporters and waste management firms also use HWIN.

Waste transporters and waste firms are parties to the e-manifest process. Like waste generators, they have a page similar to the generator's My HWIN page that allows them to complete manifest transactions and to view open and closed manifest transactions.

4.7.3.3 MOE uses HWIN to support a variety of administrative and operational functions.

MOE's field operations offices use HWIN to support inspections and compliance reviews. MOE compliance office's can, for example, use the telephonic features of HWIN to type in a license plate number of a waste hauler on a cellular phone to obtain information on the shipment (type and quantity of waste) and the carrier. Administrative functionality was built into HWIN to support MOE's financial needs. Payments collected by the HWIN system (via credit charge payments) are swept into a provincial treasury account every evening. Help desk functionality was also built into HWIN to support the need for password management, payment refunds and adjustments, and other administrative functions.

4.7.4 What service/operational problems did MOE experience during HWIN implementation?

One of the objectives that MOE had was that HWIN would replace an older legacy system. MOE used the legacy system to monitor chain of custody status of waste shipments. For each manifest transaction, MOE received the generator's and the receiver's copy of the manifest. MOE scanned each copy and entered data from each into its system. The system compared the waste/quantity information to identify discrepancies in shipments. The idea was to ensure that shipments authorized by a generator reached the receiver in full as intended.

Unfortunately, when MOE developed the specifications for HWIN, it made an assumption that all waste trading partners would shift fully to e-manifests on day one. It also assumed that the older legacy system could be immediately phased out. Both assumptions were wrong. The second assumption that the older legacy system could be discontinued created a serious problem for MOE in implementing Regulation 347. Without data that a manifest transaction had occurred and without data on the quantity of waste shipped offsite, HWIN could not calculate fees owed by waste generators. And since almost all the transactions were paper-based, HWIN had no access to transaction data.

MOE made a number of assumptions that created service or operational problems during implementation of Regulation 347.

An interface between HWIN and the older legacy system had to be rushed into production. **Figure 4.7.b** illustrates the business processes associated with the interface. Scanned images of completed manifests and manifest transaction data had to be ported over to HWIN from the legacy system daily so that HWIN could process the data, calculate fees, and present the data in HWIN.

MOE also did not appreciate the need for a help desk in implementing Regulation 347 via HWIN. About 8,000 waste generators needed to go onto the system, complete registration process and make payments in early 2002. MOE had to rush a help desk into operation to answer questions and address user issues. Many of the users needed help with password management and payment issues (refunds, credits).

4.7.5 Waste generators and waste firms did not make a move to e-manifests.

Since it was placed into operation by MOE in 2002, HWIN has performed exceptionally well as a registration and fee collection system. But, e-manifest use remains low at less than 5% of Ontario's manifest transactions.

HWIN has performed exceptionally well as a registration/fee collection system. But, only a small percentage of manifest transactions are electronic.

Low e-manifest use means that neither the Ministry of Environment or Ontario's industry are capturing available e-manifest cost benefits. In fact, by the end of 2006, Ontario's Ministry of Environment will have lost out on almost Cad\$11million in e-manifest cost savings and Ontario industry will have lost out on almost Cad\$90million in cost savings.²³

Figure 4.7.c examines root causes of low e-manifest use in Ontario and describes e-manifest lessons learned in Ontario that should be applied in the United States.

In light of the FMCSA hazmat security study, the deployment of on-board computers and wireless modem deployment by waste transporters deserves special attention. In planning for its HWIN system, Ontario officials worked under the assumption that computing capability and internet connections would be available to waste generators and waste transporters to serve the critical generator/transporter e-manifest transaction. In fact, the e-manifest process failed at the generator/transporter interface in Ontario because of the lack of internet access and computing capability at this crucial business interface. We concluded that transporters have to "bring" the computing capability and internet connection to the generator to ensure that the e-manifest process can go forward.

MOE officials wrongly assumed that computing capability and internet connectivity would be available to support the critical generator/transporter e-manifest transaction.

²³ Based on U.S. EPA e-manifest cost/benefit analyses. Lost industry cost savings 2002 – 2008 = 7 years x 200,000 manifests/year x US\$66.62 savings/manifest x Cad\$1.0/\$U.S. x 0.95 = Cad\$89million. Lost provincial cost savings 2002-2008 = 7 years x 200,000 manifests/year x US\$8.20 savings/manifest x Cad\$1.0/\$U.S. x 0.95 = Cad\$10.9million.

Figure 4.7.b MOE's paper manifest processing business process.

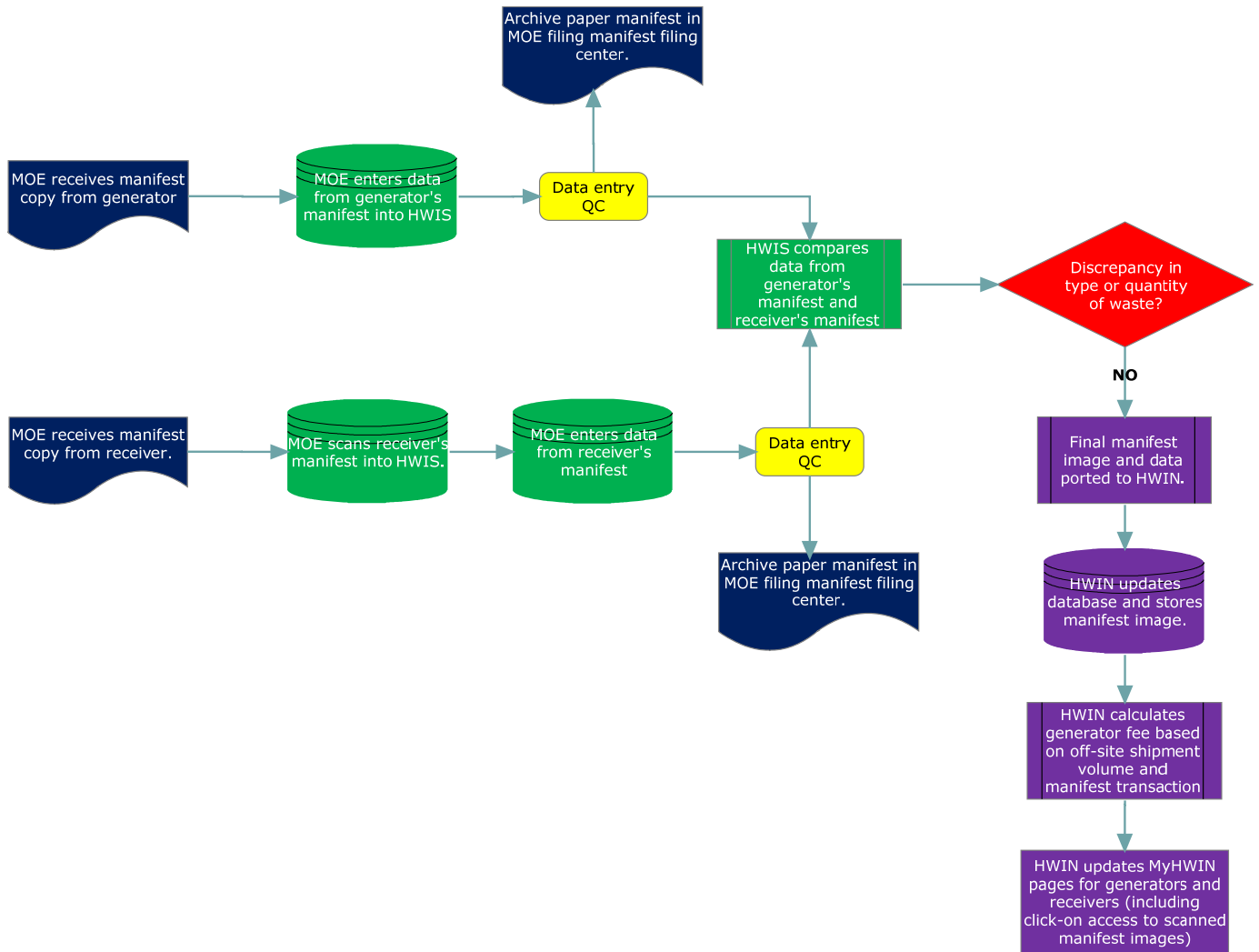


Figure 4.7.c Reasons for Low E-Manifest Use in Ontario



Waste transporters need to "bring" the internet to the generator - should be equipped with mobile computers and



Despite favorable economics, industry won't "go electronic" without a regulatory push.

Ontario E-Manifest Implementation Lessons Learned	Implementation Lessons for U.S. E-Manifest Systems
<p>The e-manifest process failed at the generator/transporter interface in Ontario because many generators do not have internet access and computing capability at the loading dock. Transporters have to "bring" the computing capability and internet connection to the generator to ensure the e-manifest process can go forward.</p>	<p>E-manifest regulations should require waste transporters to be equipped with mobile computers and wireless modems. Rationale...</p> <ul style="list-style-type: none"> • Most large waste firms have captive transport fleets. • Waste firms capture a large percentage of the e-manifest cost savings (approaching US\$50 per e-manifest). • Adding GPS with fleet tracking to mobile computing/wireless modem setup will generate net cost savings for waste firms (FMCSA study). Will enhance chain-of-custody control over waste shipments.

Industry – especially the waste industry - will not adopt e-manifests on a wide-scale operational basis without regulatory &/or financial pressure to do so. MOE did not require mandatory e-manifest use or higher fees for paper manifest transactions.	Agencies should use a regulatory “push” to promote e-manifest use. Should consider higher manifest processing fee for paper manifests (applied to waste firms)
The benefits of e-manifests are substantial – for both industry and government – but only if companies shift to e-manifests.	Cost savings for all parties, including states, cannot be captured without wide-spread e-manifest adoption by industry – arguing for goal of near 100% e-manifest use.
Regulation 347 demonstrated that hazardous waste regulatory fees offer a significant revenue opportunity for government agencies. E-manifests create cost savings that can be >> than regulatory fees. ²⁴	With state budget shortfalls, states will be interested in hazardous waste regulatory fee programs like Ontario's - especially since states can structure fee programs so that e-manifest cost savings are >> regulatory fees.
E-manifests are part of a broader set of industry & government business processes. If an e-manifest system like HWIN fails to link users' systems & processes, users will find it inefficient and difficult to adopt.	E-manifest processing systems should be XML-based, and designed to serve as the integrating link between the business processes of generators, transporters, waste firms, and government agencies.



Near 100% e-manifest adoption rate should be the objective of an e-manifest program.



E-manifest regulatory fees are viable: e-manifest cost savings can be >> industry regulatory fees.



E-manifests should be XML-based and should tie manifest business processes together.

The FMCSA hazmat security study showed that a basic “smart truck” technology package consisting of an on-board computer, GPS receiver, and wireless modem provides exceptional homeland security benefits for hazmat shipments. **Notably, this technology package will also fully meet the field deployment needs of a hazardous waste e-manifest program.** Generators and transporters can use the transporter's on-board computer and truck-based internet systems to prepare and process e-manifest transactions through an e-manifest processing center.

The basic “smart truck” technology package the FMCSA study advocates for hazmat security fully meets the field needs of a hazardous waste e-manifest program.

From an economics perspective, use of truck-based systems to support the hazardous waste e-manifest system will be efficient and cost-effective. The FMCSA hazmat security study demonstrated that hazmat fleets will capture positive ROI from “smart truck” technology deployment (see Section 1.2). And, deployment of “smart truck” technology by hazardous waste transporters will enable generators and transporters to complete e-manifest transactions and unlock e-manifest cost savings. Since the larger waste management firms in the U.S. and Canada operate captive transport fleets, waste management firms will capture the lion's share of e-manifest cost savings - about \$50 per manifest transaction. On top of positive ROI from “smart truck” technology deployment, e-manifest savings will generate huge cost savings for waste management firms.

“Smart truck” technology deployment by the waste management industry will unlock huge cost savings for the waste management industry.

4.8 The Commission for Environmental Cooperation (NAFTA Environmental Commission) envisions a North American waste tracking system.²⁵



The **North American Commission for Environmental Cooperation (CEC)** was established under the North American Free Trade Agreement (NAFTA) to promote harmonization of environmental programs between the U.S., Canada, and Mexico. The

The CEC is the NAFTA environmental commission – the United States, Canada, and Mexico support the CEC.

²⁴ Total potential benefit of e-manifests in Ontario is about Cad\$15million/year (200,000 manifests x US\$75 savings/manifest x 1.0 Cad\$/U.S.\$). Regulatory fees are Cad\$9million/year. Benefits > regulatory fees by Cad\$6million/year. B/C = 15/9=1.7.

²⁵ Home page – Commission for Environmental Cooperation: <http://www.cec.org/home/index.cfm?varlan=english>

CEC, located in Montreal, does not have any regulatory authority within the U.S., Canada, or Mexico but serves to promote the effective enforcement of environmental law, prevent trade difficulties due to environmental conflicts, and to advise the countries in managing regional/cross-border environmental issues.

U.S., Canadian, and Mexican hazardous waste regulations are similar and all three countries require hazardous waste manifests. A significant volume of hazardous waste moves between the United States and Canada with Canada being a net hazardous waste importer. Hazardous waste also moves from Mexico to the United States. Mexico lacks the commercial waste management infrastructure to manage waste, and U.S. manufacturers operating in Mexico under the Maquiladora program are required to ship the hazardous waste they generate back to the U.S.²⁶

In 2003, the CEC published a study examining the cross-border movement of hazardous waste in North America.²⁷ The study concluded that the cradle-to-grave tracking of cross-border waste shipments is not possible because environmental and customs agencies do not communicate in real time; and no country has an integrated system to electronically share data from the shipment approval process with the border inspection process.

The study also concluded that current cross-border waste tracking approaches are ineffective, inefficient, and costly. The lack of the capability to effectively track cross-border waste shipments is problematic because it creates a “hole” in North America’s cradle-to-grave regulatory system that can be exploited to hide illegal waste disposal. The study advanced a vision for a North American waste tracking approach – including use of electronic hazardous waste manifest systems – that would overcome current problems.

“...Tracking transboundary hazardous waste shipments within North America will be based on a timely electronic exchange of information which will result in improved compliance, enhanced border security, and which will minimize the administrative burden and costs to government agencies and the private sector.”

4.9 Taiwan Environmental Protection Administration – Hazardous Waste and Hazmat Shipment Tracking²⁸

Taiwan’s Environmental Protection Administration (TEPA) faced a significant problem of illegal waste disposal in the late 1990’s. Taiwan’s hazardous waste regulations are similar to U.S. regulations. For examples, waste generators must use a manifest for hazardous waste shipments.

In 2000, TEPA established the Industrial Waste Control Center (IWCC) to exercise tighter control over hazardous waste disposal – especially chain of custody control of off-site waste shipments. TEPA established an online reporting system for waste generators and in 2001 began tracking waste transporters using a GPS monitoring system.

Since then, TEPA has built the Industrial Waste Control Center into a more sophisticated operation as illustrated in **Figure 4.9.a**.

CEC study - cradle-to-grave tracking of cross-border hazardous waste shipments is not currently possible.

CEC study – e-manifest systems will enhance communication between customs and environmental agencies and enable cross-border waste tracking.

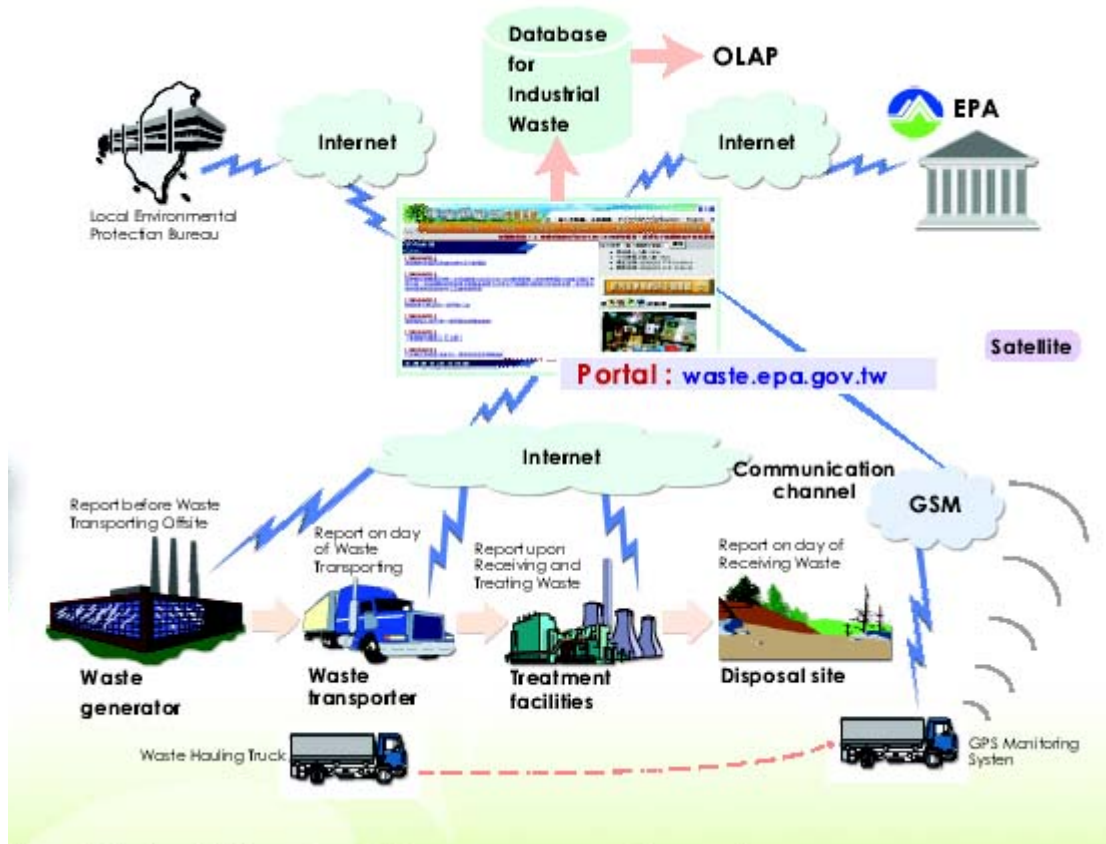
Taiwan’s environmental agency tracks the movement of waste transporters using a GPS monitoring system.

²⁶ The Maquiladora program was established as part of a treaty agreement between the U.S. and Mexico. Under the program, U.S. firms can build manufacturing plants in Mexico, ship raw products to the plants, and return finished goods to the U.S. paying only value added taxes. The program allows U.S. firms to take advantage of lower labor costs in Mexico. A provision of the treaty agreement requires the U.S. manufacturers to repatriate hazardous waste generated at Maquiladora locations in Mexico. A World Bank study estimates, however, that only about a quarter of the hazardous waste generated at Maquiladora plants is returned to U.S.

²⁷ “Crossing the Border - Opportunities to Improve Tracking of Transboundary Hazardous Waste Shipments in North America” (November 2003 - CEC) <http://www.cec.org/news/details/?varlan=english&ID=2590>

²⁸ Taiwan’s Waste Import/Export Control Measures, Taiwan Environmental Protection Administration, October 2005. <http://wm.epa.gov.tw/web/english/basel2005en.pdf>

Figure 4.9.a Taiwan's Industrial Waste Control Center



By 2005, over 15,000 firms were using the online reporting system. Over twelve million tonnes of wastes were reported through the system, accounting for 96% of all industrial wastes in Taiwan. Each day an average of over 10,000 firms submitted manifests online, and an average of over 800,000 manifests were received per month.

Recent revisions to Taiwan's Toxic Chemical Substance Transport Management Regulations by TEPA and the Ministry of Transportation and Communications will require GPS monitoring of toxic chemicals (hazmat) shipments. Class I toxic chemical tankers are required to install GPS tracking equipment by August 2008. Class II and Class III carriers are required to install GPS equipment at a later date.

According to TEPA, the objective of its monitoring program is to improve the safety of toxic chemical shipments in Taiwan and to improve response actions in the case of a spill or accident. In addition to GPS monitoring, the system will support electronic submission of manifest forms and transport routes.

Taiwan will begin tracking hazmat shipments August 2008.

4.10 How will these regulatory/legislative drivers influence the design and operation of the Transportation Security Center?

Figure 4.10.a, summarizes how regulatory/legislative drivers will influence the design and operation of the Transportation Security Center. The yellow-coded portions of the table are focused on hazmat truck tracking. Gold-coded sections focus on hazardous waste electronic manifests and green-coded sections are relevant to both hazmat and hazardous waste.

Figure 4.10.a Implications of regulatory/legislative drivers for the Transportation Security Center

**U.S. Federal Motor Carrier Safety Administration - Hazardous Materials Safety and Security
Technology Field Operational Test**

4.1

The success of the PSRC implementation approach described in the FMCSA study is dependent on voluntary technology deployment and data reporting by hazmat transporters. However, the FOT acknowledged that hazmat carriers would not likely respond to a voluntary call for technology deployment even with positive ROI.

“... Even with attractive return-on-investment (ROI) and low payback periods, capital constraints and institutional inertia (comfort with doing business in fixed ways) are likely to make penetration of this market a long-term enterprise, especially in the smaller fleet categories.”

The FMCSA study acknowledged the problem of industry-led voluntary programs by suggesting that “government intervention” (e.g. regulations) might be needed. The argument for “government intervention” is buttressed by DHS’s recent experience in its efforts to beef up security at chemical production plants in urban areas. In that case, an industry-led voluntary initiative to upgrade chemical plant security resulted in such a tepid industry response that DHS is now considering regulatory action to require chemical companies to institute security programs.

Regulations have to supply the market “push” needed to support technology deployment and data reporting – both critical to a functioning PSRC.

Almost any combination of smart truck technology can be easily and reasonably justified from a B/C perspective.

- o The cost of technology deployment/operation is low ~\$1500/truck/year (§4.1.4).
- o Wireless communications plus GPS generates overwhelmingly positive ROI due to operational efficiency gains - \$6,000-\$10,000/truck/year depending on load type (§4.1.3).
- o FOT citation - If all the hazmat carriers in the country fully deployed “smart truck” technology it would require a one-time investment of \$543 million. But, carrier profitability would rise by \$1.7 billion/year.

Operational benefits and security benefits argue for a technology package that includes: (§4.1.8)

- o Wireless communications and GPS receiver
- o Panic alert
- o Vehicle disabling
- o Electronic manifest ²⁹

Security benefits are huge arguing for wide-spread deployment of “smart truck” technology by hazmat carriers. For example, security benefits exceeding **\$5 billion** will be captured if trucks carrying bulk chemicals were equipped with GPS, wireless modems, panic alerts and remote disabling (§4.1.8).

Estimated security benefits argue for regulations that require smart truck technology deployment by 1). bulk fuel carriers; 2). bulk chemical carriers; and 3). truckload explosive carriers (§4.1.8). LTL high-hazard carriers are also a possibility.

The Public Sector Reporting Center (PSRC) was seen as a desirable mechanism for the capture and processing of data (load, location, alerts) from hazmat carriers (§4.1.9). However, the FOT study acknowledged that it is unlikely that hazmat carriers will voluntarily report data to a PSRC. Data reporting must be uniform and widespread or the security paradigm envisioned by the FOT will collapse.

Regulations must drive data reporting requirements.

The FOT participants saw value in geo-fencing as a mechanism to detect off-route shipments, and the PSRC as the point where off-route shipments would be detected. There has to be a regulatory requirement for shippers and/or carriers to submit a route report to the PSRC and a regulatory or operational mechanism for establishing geo-fences for individual shipments.

A PSRC must be able to efficiently integrate the following data on a shipment-specific basis:

1. Load and quantity data
2. Truck location
3. Transaction markers and alerts

²⁹ The electronic supply chain manifest (ESCM) was not evaluated as part of this technology configuration in the FOT. However, we envision the ESCM as the mechanism for capturing load/quantity data and driver identity information. Routing data might also be included as a feature of the electronic manifest.

4. Route information

System users will need access to web services to submit electronic shipping papers, route plans and shipment transactional data. Some data may flow from carriers' fleet tracking vendors, but some of the data must flow directly into a PSRC-managed system from the carriers' smart truck systems or from carrier corporate systems.

Geo-fencing requires establishment of routes for carriers within the system. If the shipper/carrier establishes the route, the system has to be configured to allow access. Who sets geo-fences in the system? What constitutes off-route?

Panic alerts and/or a poorly implemented geo-fence program have a significant potential for creating a high level of false positives. The system should be designed to minimize false panic alarms and/or to deal with them quickly.

Access to data on companies, personnel, and equipment will be required to make a truck tracking system work. Some of the data may exist in existing government databases. Other data may need to be collected through system registration or other mechanisms.

If regulatory fees are established, systems will be needed to process payments from companies and to remit payments to government agencies.

PSRC help desk systems are needed to support registration, regulatory assistance (?), fee payment, etc. A VOIP/CRM support system for use by help desk operators might be necessary especially if system users are interacting with the system using telephony services.

The systems that manage/support the interface between the PSRC and government action personnel are critical. For each type of incident, what are the possible support needs of the government personnel? What is the systems infrastructure that is needed to support the necessary communications between the PSRC and government agencies? Can COTS systems (like WebEOC) be integrated into system design to support the interface requirements?

To meet the needs of hazardous waste electronic manifest program, waste carriers could deploy an on-board computer and wireless communications to support e-manifest transactions – especially digital signature processing via XML webforms. The same approach might be extended to electronic processing of hazmat shipping papers and/or transaction processing. Do the commercial fleet tracking vendors currently have the hardware/software capabilities to support deployment of e-manifest solutions in the OBC-truck context?

Assume that the PSRC processes and passes incident information on to government agencies for action. Does the PSRC hold the system capabilities to fully support government incident response – for example, air dispersion modeling, hazmat medical information, etc. How would the PSRC work with government agencies in the event of an incident? Would the agencies use PSRC incident response tools to manage the incident?

There is a limit to PSRC decision support systems. Some incidents need human intervention especially to sort out low-level alerts and/or false positive alerts. The PSRC needs to be staffed by professionals that can make operational judgments about incidents as they occur.

The PSRC must operate and be staffed on a 24/7 basis. Less human intervention at the PSRC means lower staffing levels and lower PSRC costs.

Who disables a vehicle? What are the decision criteria (workflow) that have to be followed to support disabling a vehicle? FOT participants expressed a desire for a driver to be able to disable his/her vehicle.

A variable polling frequency on vehicle location (via fleet tracking vendor) needs to be triggered by different events? For example, if a truck is found to be off-route, the system should automatically ask the tracking vendor to report the vehicle's location more frequently.

The FMCSA study was silent on Federal/State implementation roles and responsibilities but there is an implied federal-lead role. A federal, 'one-size' approach to implementing a PSRC program may not provide authorized States the flexibility they want to regulate hazmat shipments on their roads.

The PSRC concept will fail without long-term funding. The FMCSA study was silent on PSRC funding sources – but the implication is that the federal government will provide long-term funding. The PSRC

	<p>concept will also fail without a regulatory push to stimulate technology deployment and data reporting.</p> <p>A truck tracking center will lessen but will not eliminate risk in the hazmat supply chain. Layers of protection need to be built into the system and its operation. For example, the ESCM will help shippers detect drivers that are not authorized to accept hazmat shipments.</p> <p>Should the hazmat ECSM and the hazardous waste e-manifest use the same technology toolset (e.g. internet XFML forms)? Should ESCM data be conveyed to the PSRC directly from the shipper/carrier or via the carrier's fleet tracking vendor?</p> <p>Should transaction events be conveyed directly to the PSRC or conveyed via the carrier's fleet tracking vendor? (ex. shipment acceptance, gate out, etc) Should all alerts be conveyed directly to the PSRC, or should some or all be conveyed through the carrier's fleet tracking vendor?</p> <p>The hazardous waste e-manifest process breaks at the generator/transporter interface because of a lack of computing capability and internet connectivity. Does a typical hazmat "smart truck" setup (OBC and wireless modem) solve this problem? Can it be used to process hazmat and hazardous waste e-manifest transactions in the field?</p>
<p>The U.S. Federal Motor Carrier Safety Administration - Untethered Trailer Tracking Systems</p>	
<p>4.2</p>	<p>The FMCSA UTT study demonstrates that UTT technology is commercially available and inexpensive to deploy. The study further demonstrated that the technology is effective. There is no technology, cost, or operational barrier to a regulation that would require carriers to deploy UTT systems.</p> <p>The communications interface will need to be modified to manage alerts and messaging associated with UTT systems.</p>
<p>U.S. Federal Motor Carrier Safety Administration – Vehicle Immobilization Systems</p>	
<p>4.3</p>	<p>The FMCSA VIS demonstrates that VIS technology is commercially available and inexpensive to deploy. The study further demonstrates that the technology is effective. The study evaluated security scenarios in which a vehicle would be disabled, and developed functional requirements for vehicle immobilization systems. There is no technology, cost, or operational barrier to a regulation that would require carriers to deploy vehicle immobilization systems.</p> <p>The communications interface will need to be modified to manage alerts and messaging associated with vehicle immobilization systems. Also, the communications interface and other systems will need to be refined to work with a concept of operations plan involving vehicle immobilization roles and responsibilities.</p>
<p>Singapore Civil Defence Force - Hazmat Transport Vehicle Tracking System</p>	
<p>4.4</p>	<p>Singapore's experience reinforces the thinking that regulations need to drive "smart truck" technology deployment. A voluntary call for technology deployment will not work.</p> <p>The SCDF views vehicle immobilization as a critical component of a hazmat security program. Given that the marginal cost of vehicle immobilization is low (FMCSA FOT) and that the SCDF experience demonstrates feasibility, vehicle immobilization should be given strong consideration in the model regulatory program.</p> <p>The SCDF's compliance experience demonstrates the need to include regulatory provisions with compliance "teeth" to ensure high compliance rates.</p> <p>The SCDF believes vehicle immobilization is an important component of a hazmat security program and designed hardware and a software interface to accommodate vehicle immobilization. The "trigger point" is an important design consideration. Does a geofence violation (encoded on the truck mounted device?) trigger vehicle immobilization?</p> <p>System should integrate OTS GIS software – chosen for cost, ease of integration and additional functionality that allows for development of web-based response tools (incident management, plume modeling, etc.)</p>

Singapore's experience shows that investment in outreach initiatives – such as pilot programs – are critical to program success.

U.S. Transportation Security Administration - Hazmat Truck Security Pilot

4.5 Congress directed TSA to undertake the HTSP project to prove that a hazmat truck tracking center was feasible and to work out the details of how a tracking center would operate. While the HTSP project was on-going, a number of important developments occurred. The FMCSA completed field testing of vehicle immobilization and untethered trailer tracking systems and the President signed into law a requirement that TSA implement a truck tracking program. DOT and DHS signed a memorandum of understanding formally shifting the responsibility for hazmat shipment security to DHS/TSA and DHS began publishing hazmat-related regulations beginning with its chemical facilities anti-terrorism standards. TSA more fully asserted its role as overseer of hazmat transportation security when it published guidance on shippers and carriers of highway security-sensitive materials on June 26, 2008. Also, DHS's Customs and Border Protection fully implemented its ACE Truck E-Manifest program that requires mandatory submission of electronic manifests for incoming truck shipments to the U.S.

The HTSP project was primarily a technology initiative. The HTSP project team was not tasked with sorting through different implementation options for a hazmat truck tracking center or for evaluating regulatory options for a hazmat truck tracking program. Instead, when the HTSP project team began its work in late 2005 it had to make assumptions about the regulatory/implementation environment in which a truck tracking system would operate. In the absence of a clear TSA regulatory plan, the project team had to assume that smart truck technology deployment and data reporting would be voluntary on the part of industry and that future TSA rules would be narrow in scope. Also, the project team assumed that states would play a passive role in protecting the hazmat supply chain – that they would react to incidents declared by TSA but would not have a hands-on role in tracking and monitoring hazmat shipments.

These assumptions – especially the assumption that technology deployment and data reporting would be voluntary - had a significant effect on the design of the HTSP prototype. The project team built limited functionality into its XML interface to the prototype because it could count on only limited data reporting by hazmat carriers and truck tracking vendors during the pilot. The business rules engine was also hobbled by a lack of data to feed it and the prototype's geo-fence functions were limited because carriers had no obligation to submit route plans. And, cargo data was limited and hard to obtain because an electronic manifest function was not built into the prototype and a number of truck tracking vendors refused to pass on shipment data to the XML interface.

A hazmat truck tracking center is dependent on data flow from shippers, carriers and truck tracking vendors. Data is the raw product that a truck tracking center converts into actionable intelligence. Efficient and timely processing of data gives the center the ability to function and allows it to effectively support government action agencies when a transportation security incident is declared. However, a truck tracking center will fail unless smart truck technology is widely deployed and shippers, carriers and truck tracking vendors submit data to the truck tracking center. Currently, there is no regulatory requirement that hazmat shippers deploy smart truck technology or submit data to a truck tracking center. In the HTSP, carriers and truck tracking vendors were unwilling to voluntarily submit the full set of data needed to make a truck tracking center work. And, many felt that the program should be voluntary only – not unlike the chemical industry's reaction to DHS's chemical plant security initiative. The HTSP contractor expended a great deal of effort doing "work arounds" because the data it received from carriers and truck tracking vendors was inconsistent and incomplete. In fact, the HTSP contractor was able to implement only a small part of the functionality that a truck tracking center needs to deliver because of the paucity of the data it was able to get from carriers and truck tracking vendors. A national truck tracking program will fail if this is not remedied. Regulations need to require technology deployment and data reporting. The regulations need to be specific about technology standards and data reporting standards.

The HTSP program proved that a hazmat truck tracking center is technically feasible and that smart truck technology can be crafted into an effective and efficient system for tracking hazmat shipments. The design of the truck tracking prototype in the HTSP is sound and integrates most of the building blocks of a truck tracking center (see Section 4.5.1). However, the prototype lacks the full functionality needed in a truck tracking center – especially considering regulatory and programmatic developments that occurred after the HTSP program began in October 2004.

The concept of operations (ConOps) plan developed by the HTSP project team did not have a role for state action agencies, failing to reflect the possibility of a stronger implementation role for states in protecting the hazmat supply chain.

The ConOps plan developed by the HTSP project team did not reflect the regulatory approach that will likely be implemented by TSA and the states.

The ConOps plan developed by the HTSP project team also did not reflect the full set of responsibilities that will face shippers, carriers and truck tracking vendors when a truck tracking center with full functionality is implemented. For example, the pilot did not factor in vehicle immobilization, untethered trailer tracking, electronic routes or electronic manifests. The ConOps plan will need to change to reflect a more sophisticated mix of tracking center functionality.

The HTSP report acknowledged the need for better interaction between the truck tracking center and TSA. Beyond this, the truck tracking center needs to coordinate events and information flow with state fusion centers and local governments. COTS web-based crisis information management software (CIMS) would probably be the most efficient and effective approach to meeting this need. An added benefit of most CIMS is that it supports management and operations of a command center (e.g. truck tracking center). Section 3.9 describes CIMS by highlighting a market leading product – WebEOC™.

U.S. Customs & Border Protection – ACE Truck E-Manifest

4.6 The ACE Truck E-Manifest program is a huge regulatory precedent.

- o It covers all carrier-based shipments from Canada and Mexico in the U.S. (including hazmat and hazardous waste).
- o At the heart of the ACE program is the electronic manifest. ACE uses an electronic manifest to capture information on trading partners, trucks/equipment, and load (type and quantity). The Transportation Security Center will also use an e-manifest to capture information.
- o Regulations make participation mandatory. CBP regulations require trucks entering the U.S. to submit an electronic manifest. They also require carriers to install on-board equipment.
- o The Truck E-Manifest program and the Transportation Security Center overlap on some shipments (hazmat and hazardous waste).
- o CBP and TSA are both DHS agencies.

CBP's Truck E-Manifest program is a clear precedent for requiring technology deployment and data reporting from the transportation industry.

Regulatory integration between the CBP's Truck E-Manifest program and TSA's hazmat truck tracking program should be a goal between CBP and TSA.

Section 4.6.2 lists the data elements that the CBP's Truck E-Manifest captures for every shipment. The TSA e-manifest will need some of the CBP's data elements and others in addition. CBP and TSA should develop a list of common/additional data elements and coordinate e-manifest processing. For example, an e-manifest for a shipment of hazardous materials filed through CBP's portal should flow directly into the Transportation Security Center and should have all the data elements needed to meet TSA truck tracking requirements.

CBP uses web services to accept electronic manifests. The Transportation Security Center will also use web services to accept electronic manifests. However, the hazmat truck tracking center may be taking in more data (vehicle location, e-manifest, e-route) from more sources (shippers, carriers, truck tracking vendors). The approach is similar but the technical challenge for hazmat truck tracking is greater.

CBP's Truck E-Manifest program uses a business rules engine to evaluate shipments before they reach the border. The hazmat truck tracking system will also use a business rules engine as a dynamic risk profiling tool. Some of the rules for evaluating companies and drivers may be similar between the programs.

Ontario Hazardous Waste Information Network

4.7 Near 100% hazardous waste e-manifest use should be the objective of an e-manifest program – otherwise, industry and government miss out on cost savings.

	<p>Industry will not make a wide-scale shift to hazardous waste e-manifests without regulatory and/or financial pressure. Without a regulatory push to overcome market inertia, most companies will stay with paper manifests.</p> <p>Hazardous waste e-manifest regulatory fees are viable, especially since states can deliver e-manifest costs savings to industry that are far greater than industry-paid regulatory fees.</p> <p>The hazardous waste e-manifest process will fail at the generator/transporter interface unless there is internet connectivity and computing capabilities available to the parties. Waste transporters should be equipped with an on-board computer and wireless modem to 'bring' the internet and computing power to the critical generator- transporter hazardous waste e-manifest transaction.</p> <p>A hazardous waste e-manifest system links the business processes of waste generators, waste haulers, and waste firms. It has to allow user data to flow efficiently through the system to support external business processes as well as meeting its own internal e-manifest business processes. There should be defined XML interfaces created that allow system users to efficiently link to the e-manifest system.</p> <p>Based on the experiences in Ontario in implementing its hazardous waste e-manifest system, help desk systems need to be established that support system user needs fully and efficiently.</p>
Commission for Environmental Cooperation (NAFTA Environmental Commission)	
4.8	<p>Hazmat and waste tracking systems will need to be built to serve the tri-lingual needs of North American customers.</p> <p>The NAFTA environmental commission has backed establishment of a North American waste tracking system. The commission has no regulatory authority but does speak for the common interests of the United States, Canada, and Mexico.</p>
Taiwan Environmental Protection Administration - Hazardous Waste and Hazmat Shipment Tracking	
4.9	<p>Taiwan EPA requires hazardous waste transporters to install GPS monitoring equipment on their trucks. The purpose is to strengthen chain of custody control over hazardous waste shipment and to prevent illegal waste disposal. Should the model regulation also require tracking of hazardous waste shipments to strengthen chain of custody control in the U.S.?</p> <p>Taiwan requires submission of electronic manifests for hazardous waste shipments to its Industrial Waste Control Center. Unlike Ontario, where e-manifest use is voluntary and e-manifest usage is low, almost all of Taiwan's transactions are electronic.</p> <p>Taiwan is about to begin tracking hazmat shipments. Notably, Taiwan requires submission of e-manifests (type, quantity of load) and electronic route information and GPS monitoring of hazmat carriers (location). Taiwan had combined the interests of two agencies with different regulatory focus – environment and transportation – to build an efficient regulatory program that meets multiple interests.</p>



5.0 Business Drivers

Business drivers are external or internal influences that significantly impact or set direction for programs. Sections 2-4 examined in detail the wide array of events in the market that will influence the establishment and operation of the Transportation Security Center. Section 5 begins to tie together the analyses conducted in Sections 2-4 by listing business drivers that will likely impact or set the direction for a hazmat truck tracking and hazardous waste e-manifest processing.

5.1 Hazmat shipment tracking – the top five business drivers

5.1.1 The 9/11 Commission Act of 2007 (PL 110-53/H.R. 1) requires TSA to take action on hazmat truck tracking.

As discussed in Section 2.5, PL 110-53 requires TSA to:

...develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides--

(A) frequent or continuous communications;

(B) vehicle position location and tracking capabilities; and

(C) a feature that allows a driver of such vehicles to broadcast an emergency distress signal.

A legislative mandate is a powerful incentive for a federal agency. TSA's objective should be to open an operational hazmat truck tracking center as soon as possible – especially since earlier studies and initiatives have proven that a truck tracking center is technically feasible. In its June 26, 2008 guidance, TSA signaled its interest in applying stringent security measures for TSA-designated Tier 1 highway security-sensitive materials (HSSMs). This focuses tracking scrutiny down to a small percentage of the universe of hazmat shipments.

5.1.2 There is public demand for a secure hazmat supply chain.

There have been attacks using truck-based hazmat shipments around the world and the U.S. public fears that hazmat shipments could be used as weapons of mass destruction here in the United States. In Kentucky, for example, the former Director of the Kentucky Office of Homeland Security reported that hazmat truck security was raised as a pressing issue by Kentucky citizens in every public forum she attended. The public recognizes hazmat supply chain security as a national issue and wants TSA to act as soon as possible – and certainly before an actual incident occurs.

5.1.3 Security is driving technology innovation in the hazmat truck security market; the market anticipates a government regulatory program.

Section 2.2 explained how hazmat security issues are driving the regulatory agenda for government agencies with a transportation mandate. Section 3.1 described "smart truck" technology and included a review of the commercial "smart truck" products available in the market. Section 4.2-4.3 reviewed additional "smart truck" technology devices.

The market anticipates that government regulation will eventually dictate the deployment of "smart truck" technology in segments of the hazmat transportation market. Product development by "smart truck" technology vendors has increasingly focused on developing product security features, and product marketing has increasingly emphasized hazmat shipment security.

Two examples highlight the market's recognition of hazmat security as a market.

- Section 3.2 described the Chemical Custody Supply Chain Solution, an application that provides continuous on-line tracking, security monitoring and management of hazardous material containers and their contents from point of origin to destination. It is offered by Savi/Lockheed (Savi). Savi was one of the first technology vendors to emphasize hazmat security as an important,

if not the chief, benefit of its product. Savi's message reflects the market's readiness for products and services that address the threat of terrorist actions in the hazmat supply chain. Benefits cited by Savi include:

- reduced liability risk;
- increased security;
- streamlined operational processes;
- reduced asset inventory; and
- reduced capital investment, lease, rental, and demurrage costs.

• Sections 3.1 described the product offerings of Safefreight Technology. Safefreight is notable in that it has aligned its "smart truck" products around hazmat transportation security. A visit to Safefreight's webpage demonstrates the company's recognition that the hazmat transportation security market is fast arriving.

<http://www.safefreight.com/security-by-technology/hazmat-security-technologies/>

5.1.4 "Smart truck" technology deployment saves hazmat carriers money; generates huge benefits for the public.

Section 4.1 examines the cost/benefit of hazmat truck tracking programs. It is overwhelmingly evident that there is a clear cost argument for requiring hazmat carriers – especially high-risk hazmat carriers - to deploy "smart truck" technology.

o The cost of technology deployment/operation is low ~\$1500/truck/year (§4.1.4).

o Wireless communications plus GPS generates overwhelmingly positive ROI due to operational efficiency gains - \$6,000-\$10,000/truck/year depending on load type (§4.1.3).

o If all the hazmat carriers in the country fully deployed "smart truck" technology it would require a one-time investment of \$543 million but carrier profitability would rise by \$1.7 billion/year.

There is also a clear benefits argument as well. The FOT report concluded that security benefits exceeding **\$5 billion** will be captured if trucks carrying bulk chemicals were equipped with GPS, wireless modems, panic alerts and remote disabling (§4.1.8).

The cost savings/benefits of "smart truck" technology deployment will create a great deal of flexibility for federal and state regulatory agencies. The overwhelmingly positive ROI on "smart truck" investment should mute concerns by hazmat carriers that regulatory requirements for technology deployment and data reporting are burdensome. Also, the social benefits are so great that concerns over regulatory burden elsewhere in the hazmat supply chain can be easily mitigated.

5.1.5 Technology is not an inhibiting factor for a truck tracking center; developing an effective regulatory/implementation framework is the challenge.

TSA's Hazmat Transportation Security Pilot program proved that a hazmat truck tracking center is technically feasible and that smart truck technology can be crafted into an effective and efficient system for tracking hazmat shipments. And, it is clear that technology vendors have the capability to refine their products to meet the government's needs for a national truck tracking system.

Technology will not be an inhibiting factor for a truck tracking center. The challenge in establishing a truck tracking center will be in developing the regulatory and implementation paradigm in which it will operate. And those that do will be in the lead position to place a truck tracking center into operation.

5.2 Hazardous waste e-manifests – the top five business drivers.

- 5.2.1** EPA wants hazardous waste trading partners to use e-manifests. | Section 2.6 describes EPA's multi-year effort to try to implement an e-manifest program. Despite its inability to date to implement an e-manifest program, EPA remains firmly committed – even to the point of supporting legislation that would allow it to move forward on a privatization plan to implement a national e-manifest processing center. And, EPA's support and leadership is critical. Until EPA allows companies and states to use e-manifests, they remain bound to the current costly and inefficient paper-based system.
- 5.2.2** E-manifests will unlock cost savings for government and industry. | With about 4 million hazardous waste shipments in the U.S. each year, EPA estimates electronic manifests have the potential to generate savings of more than \$300 million per year. This translates into cost savings of about \$75/manifest transaction. Waste transporters and waste management firms together capture about two-thirds of available e-manifest cost savings – about \$50/manifest transaction. Waste generators and state agencies capture the remainder. The waste management industry operates under thin margins, and will welcome e-manifest cost savings. Many states and waste generating companies likewise face serious economic pressures and will happily embrace cost savings from e-manifests.
- 5.2.3** E-manifest cost savings provide revenue opportunity for state agencies. | Cash strapped states are increasingly looking for revenue opportunities. Kentucky, like many other states, currently has regulations in place that require waste generators to pay fees based on waste generation. Section 4.7 described how the Province of Ontario crafted a regulatory fee program to generate CAD\$10 million/year in revenue. With the inherent cost savings associated with e-manifests (e.g. \$75/transaction), there is plenty of room for a state to collect regulatory fees and still deliver a benefit to regulated companies. For example, Section 4.7 examined Ontario's fee program. Even with Ontario's extremely hefty regulatory fee structure, e-manifests offer a healthy benefit/cost value proposition.
- With about 200,000 manifest transactions/year, the use of e-manifests instead of paper manifests has the potential of generating US\$15 million in annual cost savings (200,000 x \$75) in Ontario. Ontario collects about CAD\$9 million/year (US\$10.2 million) in regulatory fees from waste generators. Assuming full e-manifest use, the benefit/cost ratio for an e-manifest program in Ontario is ~1.5 (B=\$15million; C=\$10.2 million). This is an impressive B/C ratio considering the heavy regulatory fee burden Ontario places on waste generators.
- 5.2.4** Hazardous waste management is a state-delegated program. | The states - not EPA - oversee hazardous waste management programs in the U.S. The states are the regulatory point of contact for companies and the states are responsible for compliance/enforcement actions. States have been traditionally forceful about maintaining their role in managing their hazardous waste programs. For example, the Alliance for Uniform Hazmat Transportation Procedures, sponsored by the National Conference of State Legislatures, has established model programs for hazardous waste transportation. The states are a key partner with EPA and will significantly influence the implementation of hazardous waste e-manifest programs. Given the revenue

potential associated with e-manifest implementation, the states will likely have an especially keen interest in how the program is structured.

5.2.5 Technology is not an inhibiting factor for a hazardous waste e-manifest processing center; developing an effective business, regulatory, and implementation framework is the challenge.

Like the truck tracking center, technology is not an inhibitor to the establishment of a hazardous waste e-manifest processing center. In fact, technology can substantially expand shipment chain-of-custody control far beyond EPA's current objective for its e-manifest program. Section 3 reviewed technology that will support an e-manifest system and Section 4.7 reviewed Ontario's Hazardous Waste Information Network, the only hazardous waste e-manifest system in North America.

Technology will not be an inhibiting factor for a hazardous waste e-manifest processing center. As EPA has discovered over the years, the challenge in establishing an e-manifest processing center will be in developing the business, regulatory and implementation paradigm in which it will operate. And those that do will be in the lead position to place an e-manifest processing center into operation.

5.3 Business drivers common to both hazmat shipment tracking and hazardous waste e-manifests.

5.3.1 The transportation of hazardous materials and hazardous waste is a highly regulated business.

Regulation is a clear business driver for the transportation industry. Regulations from EPA and DOT cover hazardous waste transportation safety and place strict requirements on hazardous waste trading partners (generators, transporters, waste firms). Regulations from DOT and TSA cover hazmat transportation safety and security and place strict requirements on hazmat trading partners (shippers, carriers, receivers). As noted in two previous sections, regulation will inevitably drive the adoption of "smart truck" technology by hazmat carriers and the use of e-manifests by hazardous waste trading partners. The nature and type of regulations that are ultimately adopted will shape the market for hazmat shipment tracking and hazardous waste e-manifests.

5.3.2 EPA's proposed transaction revenue model supports establishment of a for-profit business for hazmat shipment tracking and hazardous waste e-manifest processing.

EPA's "share-in-savings" business model calls for a private company to build and operate an e-manifest processing center. The company will collect a transaction fee for each hazardous waste electronic manifest it processes. A business model based on transaction fee revenues will work equally well for hazmat shipments, and can be extended to a for-profit approach for establishing a hazmat truck tracking center. In the hazmat case, the transaction would begin at "gate out" and would end at "gate in". The fee paid would be for tracking services from "gate out" to "gate in".

5.3.3 Government agencies are interested in privatization – especially when intramural funding is limited.

The Congressional Research Service defines "privatization" as *the use of the private sector in the provision of a good or service, the components of which include financing, operations (supplying, production, delivery), and quality control.*¹ Government agencies are most interested in privatization when the performing organization: 1). can do the work less expensively than the government; 2). will deliver high service quality; and 3). advances a business model that lessens an agency's downstream financial obligations. EPA's interest in the GSA "share-in-savings" contract mechanism is an excellent example of government privatization

¹ Privatization and the Federal Government: An Introduction; Congressional Research Service; December 28, 2006.

| (refer to Section 2.6.3).

5.3.4 Financial considerations and programmatic/technology overlaps argue for co-location of TSA's hazmat truck tracking center and EPA's hazardous waste e-manifest processing center.

As explained in Section 2.1, there are programmatic overlaps between hazardous materials and hazardous waste. Hazardous waste is a subset of the much larger universe of hazardous materials, and EPA and DOT co-regulate the hazardous waste transportation (EPA does not, however, regulate the transportation of hazardous materials other than hazardous waste). The systems infrastructure needs for a hazmat truck tracking system and a hazardous waste e-manifest processing center are similar, and significant economies of scale can be achieved if TSA's hazmat truck tracking center and EPA's hazardous waste e-manifest processing center are co-located.



6.0 Regulatory Program Plan

This section contains recommendations for two model regulatory programs for consideration by Kentucky cabinet agencies. The first is a model program to support implementation of TSA's hazmat truck tracking program. The second is a model program to support implementation of EPA's hazardous waste e-manifest program.

Section 6.1 begins by providing an analysis of terrorist threats to Kentucky's hazmat supply chain including shipments of hazardous materials by truck. Section 6.2 contains project team recommendations for Kentucky's membership in the Alliance for Uniform Hazmat Transportation Procedures. Section 6.3 describes the regulatory strategy that would drive the model programs, and Section 6.4 presents critical regulatory elements of the model programs. Section 6.5 presents recommendations for refinements to Kentucky's existing hazmat and hazardous waste regulatory programs.

6.1 Kentucky's hazmat supply chain is an attractive target for terrorists.

Appendix F, Kentucky Hazmat Supply Chain Threat Analysis, contains a report that describes terrorist threats to Kentucky's hazmat supply chain including shipments of hazardous materials by truck.

Kentucky is located in the middle of one of the nation's busiest transportation corridors. Major interstate highways including I-64, I-65, and I-75 cut through the state carrying over 70,000 semi-tractor trailer trucks daily. In fact, only six states have more truck tonnage over their roads than Kentucky.

The study advanced the idea that Kentucky might serve as a "magnet" for out-of-state terrorists seeking the significant stores of hazardous materials at petrochemical complexes in Louisville, and in eastern and western Kentucky or seeking to divert a hazmat shipment in-route on Kentucky's roads. The materials could be transported out of state for use elsewhere or used as weapons of mass destruction at large, high-profile sporting venues like the Kentucky Derby.

The report concluded that Kentucky's hazmat supply chain – including carrier-based transportation – was an attractive target for terrorists.

Kentucky's hazmat supply chain is an attractive target for terrorists.

6.2 Kentucky should seek membership in the Alliance for Uniform Hazmat Transportation Procedures

Responsibility for hazmat and hazardous waste programs has been delegated to Kentucky by EPA and DOT. Kentucky's hazmat program incorporates DOT regulations by reference while its hazardous waste program has been enhanced beyond EPA-minimum requirements to include items such as regulatory fees for waste generators. See Section 6.5 for additional detail.

Section 2.7 described the Alliance for Uniform Hazmat Transportation Procedures (the Alliance), a state-based organization that operates in conjunction with the National Conference of State Legislatures (NCSL). The Alliance has developed model hazmat and hazardous waste registration/permitting programs that its member states use as guides for in developing their own regulatory programs. Kentucky is bordered by three Alliance states – West Virginia, Ohio, and Illinois.

Membership is open to all states but candidate states must satisfy membership requirements to join the Alliance (See Section 2.7.3). Section 2.7.5 listed benefits of state membership in the Alliance.

- *The Uniform Program is well designed, comprehensive, and has stood the test of time.* The Alliance has developed detailed procedures to support state implementation of the Uniform Program. The Alliance procedures have been

The Alliance for Uniform Hazmat Transportation Procedures is a state-based organization that operates in conjunction with the National Conference of State Legislatures (NCSL).

developed and refined by almost two decades of state experience. The procedures have a proven track record work in minimizing administrative burdens of the states in implementing their base programs.

Membership in the Alliance for Uniform Hazmat Transportation Procedures will deliver substantial benefits to a state.

- *Membership in the Alliance makes it easier for states to implement and defend fee programs to fund internal programmatic activities.* States need revenue to run their programs, and the Alliance program is structured to allow states to capture fees from hazmat carriers in a defensible, reasonable manner. Participation in the Alliance program also helps state administrators justify the collection of hazmat fees.
- *Carrier compliance is enhanced and highway safety/security is improved.* The Alliance reports that carrier compliance with hazmat safety rules is markedly improved by implementation of the Alliance program.
- *Less workload and efficient business processes save states money.* Alliance membership helps states share the workload. Instead of registering and reviewing every hazmat carrier in their state, states only register and review those carriers that identify a given state as their base state. This allows each state to focus their attention and resources on a smaller group of carriers without losing confidence that other carriers are also being thoroughly checked. Base states are able to improve the thoroughness of carrier reviews and inspection and capture cost savings from the decreased volume of registration and reviews required.
- *Lower regulatory load for interstate hazmat carriers.* Interstate carriers benefit from the Alliance program. Instead of having a regulatory interaction with many states, carriers interact with only their base state for permitting and registration. A lighter regulatory load lowers carrier costs.

In June 2008, the Alliance issued a contract to better quantify the benefits of Alliance membership. The work is not yet complete but will provide states with additional information to evaluate the benefits of Alliance membership.

Kentucky should seek membership in the Alliance for Uniform Hazmat Transportation Procedures

The project team recommends that Kentucky seek membership in the Alliance for Uniform Hazmat Transportation Procedures. Membership in the Alliance places Kentucky in position to host the North American Transportation Security Center. The Alliance base program is consistent with the statutory/regulatory refinements Kentucky needs to make to implement its model hazmat truck tracking program and its model hazardous waste e-manifest program. The Alliance program also lets Kentucky cabinet agencies collect regulatory fees to cover internal programmatic costs. The administrative burden on the Cabinet agencies in adopting Alliance programs will be low and the benefit to Kentucky carriers, especially interstate carriers, will be high.

The Kentucky Transportation Cabinet should serve as the lead agency in Kentucky, and Kentucky should opt to register/permit all hazmat carriers including hazardous waste carriers.

6.3 Recommended regulatory strategy

This project is being conducted as part of an overall plan to bring two federal initiatives to Kentucky: TSA's hazmat truck tracking center and EPA's hazardous waste e-manifest processing center. Bringing these programs to Kentucky will create well-paying technology jobs and provide a welcome economic boost to Kentucky's 5th Congressional district.

The North American Transportation Security Center will be the implementing tool for a model regulatory program.

The North American Transportation Security Center will be the implementing tool for a model regulatory program that will require:

- high-risk hazmat transporters to install "smart truck" technology on their vehicles;
- carriers to process hazmat e-manifests through the Transportation Security Center;
- carriers to report vehicle location to the Transportation Security Center (real-time XML data feed); and
- companies to pay hazmat regulatory fees.

The Transportation Security Center will also serve as the implementing tool for a model hazardous waste electronic manifest regulatory program.

The strategy behind the model regulatory program has to reflect state and federal needs as well as the business needs of the Transportation Security Center.

The project team adopted the following strategy as it crafted its regulatory recommendations for consideration by Kentucky's cabinet agencies.

6.3.1 Kentucky's model program will support implementation of PL 110-53 (Tier 1 HSSM tracking).

The model regulatory program will focus on tracking TSA-designated Tier 1 Highway Security-Sensitive Materials (HSSM). Tier 1 HSSM shipments represent less than 1% of all hazmat shipments. The Transportation Security Center will operate a hazmat truck tracking center for Tier 1 HSSMs that will fully satisfy the implementation needs of PL 110-53 and that will serve as the implementing tool for a model hazmat shipment tracking program. The hazmat shipment tracking program recommended for Kentucky will serve as a model program for states and/or a model for future TSA regulations.

6.3.2 Kentucky's model program will support implementation of EPA's hazardous waste e-manifest program.

The model regulatory program will be developed consistent with EPA's hazardous waste e-manifest program. The Transportation Security Center will operate a hazardous waste e-manifest processing center that will be CROMERR-compliant and that will serve as a node on EPA's Central Data Exchange. The hazardous waste e-manifest program recommended for Kentucky will serve as a model program for states and/or a model for future EPA regulations.

6.3.3 Kentucky's model program will position Kentucky to host the Transportation Security Center and establish the Transportation Security Center as a for-profit business.

By being in the regulatory/business forefront, Kentucky will position itself to serve as host of the Transportation Security Center. Model regulations will be developed with the idea that the Transportation Security Center will serve as the implementing tool for the regulations. The Transportation Security Center will process hazmat and hazardous waste transactions from states and provinces throughout North America.

6.3.4 Kentucky's model program will support Kentucky's entry into the Alliance for Uniform Hazmat Transportation Procedures.

Section 2.7 described the procedures and policies that underlie the Alliance for Uniform Hazmat Transportation Procedures. The base program is comprehensive and compatible with the technical and programmatic goals of the North American Transportation Security Center. Section 6.2 included a recommendation that Kentucky join the Alliance. The model program developed in Kentucky will incorporate Alliance registration/permitting provisions.

6.4 Critical elements of the model regulatory programs.

Sections 2, 3, and 4 analyzed "drivers" that will influence the design and operation of the Transportation Security Center. Section 2.8 summarized the implications of regulatory/legislative drivers on the design and operation of the Transportation Security Center. Section 3.11 summarized technology drivers and Section 4.10 summarized experience drivers.

These "drivers" also have a profound effect on the design of regulatory programs related to hazmat truck tracking and hazardous waste electronic manifests. One issue that arose frequently during the course of this project was that voluntary industry compliance programs do not work. For example, DHS's industry voluntary program for chemical plant safety met with such tepid response by industry that DHS was forced to issue its Chemical Facility Anti-Terrorism Standards regulations to require chemical facilities to institute hazmat security programs. In order for hazmat truck tracking and hazardous waste e-manifest programs to work, they need a high level of industry participation. The model programs recommended by the project team will apply regulatory and financial incentives to promote technology deployment, data reporting, and e-manifest use by industry.

Regulations need to drive technology deployment, data reporting and electronic manifest use.

This section describes critical elements of the model regulatory programs that would be implemented in conjunction with the Transportation Security Center.

6.4.1 Tier 1 HSSM shipment tracking

A hazmat truck tracking center is dependent on data flow from shippers, carriers and truck tracking vendors. Data is the raw product that a truck tracking center converts into actionable intelligence. Efficient and timely processing of data gives the center the ability to function and allows it to effectively support government action agencies when a transportation security incident is declared. However, a truck tracking center will fail unless "smart truck" technology is widely deployed and shippers, carriers and truck tracking vendors submit data to the truck tracking center. Currently, there is no regulatory requirement that hazmat shippers deploy "smart truck" technology or submit data to a truck tracking center. In TSA's Hazmat Truck Security Pilot, carriers and truck tracking vendors were unwilling to voluntarily submit the full set of data needed to make a truck tracking center work. And, many felt that the program should be voluntary only – not unlike the chemical industry's reaction to DHS's chemical plant security initiative. The HTSP contractor expended a great deal of effort doing "work arounds" because the data it received from carriers and truck tracing vendors was inconsistent and incomplete. In fact, the HTSP contractor was able to implement only a small part of the functionality that a truck tracking center needs to deliver because of the paucity of the data it was able to get from carriers and truck tracking vendors. A national truck tracking program will fail unless regulations drive technology deployment and data reporting. Moreover, regulations need to drive technology standards and data reporting standards.

A hazmat truck tracking center will fail unless carriers deploy "smart truck" technology and submit data.

PL 110-53 and TSA's HSSM guidance establish the framework for a regulatory framework for technology deployment and data reporting.

The HTSP program proved that a hazmat truck tracking center is technically feasible and that smart truck technology can be crafted into an effective and efficient system for tracking hazmat shipments (see Section 4.5.1). However, the HTSP study stopped well short of describing a regulatory program that would promote the successful establishment of a hazmat truck tracking program.

PL 110-53 and TSA's June 2008 guidance for Highway Security-Sensitive Materials do, however, establish the framework for a regulatory program that would promote technology deployment and data reporting. The regulatory elements listed below are designed to support implementation of PL 110-53 and field implementation of TSA's HSSM guidance. They focus regulatory scrutiny on Tier 1 HSSMs, and promote "smart truck" technology deployment and data reporting by Tier 1 HSSM shippers and carriers.

6.4.1.1 Shipments of TSA-designated Tier 1 highway security-sensitive shipments (HSSMs) are "regulated shipments".

There are 800,000 hazmat shipments per day in the United States – over 290 million shipments annually. Not all materials represent the same risk during transit, especially from a security perspective. In its June 26, 2008 guidance, TSA recognized two tiers of highway security-sensitive materials.

1. **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.
2. **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. A full list of Tier 2 HSSM may be found in **Appendix B**.

As discussed in Section 2.4, TSA also published voluntary Security

Action Items (SAIs) for Tier 1 and Tier 2 HSSMs. They include the following SAIs for en-route security.





10. Establish Communications Plan.
11. Establish Appropriate Vehicle Security Program.
12. Establish Appropriate Cargo Security Program.
13. Implement a Seal/Lock Control Program.
14. High Alert Level Protocols.
15. Establish Security Inspection Policy and Procedures.
16. Establish Reporting Policy and Procedures.
17. Shipment Pre-Planning, Advance Notice of Arrival, and Receipt of Confirmation Procedures.
18. Preplanning Routes.
19. Security for Trips Exceeding Driver Hours of Service.
20. Dedicated Truck.
21. Tractor Activation Capability.
22. Panic Button Capability.
23. Tractor and Trailer Tracking Systems

SAIs 17-23 are recommended by TSA for Tier 1 HSSM shipments.

Figure 6.4.a lists Tier 1 HSSMs and the number of annual shipments of each HSSM. At less than 2 million shipments per year, Tier 1 HSSM shipments represent well less than 1% of all hazmat shipments in the U.S. This is a reasonable number of shipments to track, and focuses government attention on the riskiest shipments from a security perspective.

The model regulation requires shippers/carriers of Tier 1 HSSMs to implement a truck tracking program. For purposes of this paper, Tier 1 HSSM shipments are referred to as **“regulated shipments”**.





Figure 6.4.a TSA Tier 1 Highway Security Sensitive Materials

DOT Hazard Class	Hazmat Placard	Threshold Quantity	Number of Annual U.S. Shipments ¹
Division 1.1 Division 1.2 Division 1.3 Explosives		Any quantity	Domestic - 11,868 NAFTA - 524
Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation)		Anhydrous ammonia (UN1005) in single bulk packaging >300 L or 3000 kg	Domestic - 563,771 ² NAFTA - 6,767
Division 2.3 Toxic (Poison) Gas		Hazard zone A & B >5lbs. in a single package Hazard zone C & D in single bulk packaging >3000L or 3000kg	Domestic - 960,871 NAFTA - 8,233
Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation)		PG I in single bulk packaging > 3000 L or 3000 kg	Domestic - 62,015,889 ³ NAFTA - 119,816

¹ Data on the number of Tier 1 HSSM shipments was provided by David Cooper, Program Manager, Highway & Motor Carrier Division, U.S. Transportation Security Administration. Data represents 2005 projections for US domestic and NAFTA truck traffic for select hazmat commodities.

² This figure includes shipments of Tier 2 Division 2.2 Non-Flammable Gases (subsidiary hazard Oxidizer Division 5.1).

³ This figure includes shipments of : 1). Class 3 Flammable Liquids (PGI and II in single bulk packaging > 300L or 3000 kg; and 2). Class 3 Flammable Liquids (any quantity desensitized explosives) – both of which are Tier 2 HSSM.

Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)		Hazard zone A & B > 5 lbs. in a single package	Domestic - 307,244 NAFTA - 18,213
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)		Hazard zone C & D in single bulk packaging > 3000 l or 3000 kg	
Class 7 Radioactive Materials		IAEA Code of Conduct Category 1 and 2 materials including Highway Route Controlled quantities as defined in 49 CFR 173.403 or known as radionuclides in forms as RAM-QC by the Nuclear Regulatory Commission	Domestic - 7,777 NAFTA - 7,265
Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation)		Packing group I and II in single bulk packaging > 3000 L or 3000 kg	Domestic - 4,548,595 ⁴ NAFTA - 95,703
Other Materials		Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules.	unknown
			Domestic - 1,287,760 ⁵

6.4.1.2 Tier 1 HSSM shipments traveling over Kentucky's roads must meet Kentucky's hazmat shipment security requirements.

Regulated shipments that travel over Kentucky's roads are subject to Kentucky's hazmat security regulatory requirements. The requirements are spelled out below.

6.4.1.3 Carriers of Tier 1 HSSM shipments must install "smart truck" devices that are Transportation Security Center compliant.

Compliance with Tier 1 HSSM requirements requires "smart truck" technology deployment by Tier 1 HSSM carriers. In its June 26, 2008 guidance, TSA published 23 Security Action Items (SAIs) for Tier 1 HSSMs. SAIs 17 – 23 cover en-route requirements for Tier 1 HSSMs. SAIs 21, 22, and 23 specifically address the deployment of "smart truck" technology on vehicles carrying Tier 1 HSSMs.

- **Security Action Item #21. Tractor Activation Capability** – 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.
- **Security Action Item #22. Panic Button Capability** – 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.
- **Security Action Item #23. Tractor and Trailer Tracking Systems** – 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. Geo-fencing 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

⁴ This figure includes shipments of Class 8 Corrosive Materials (Packing group I in single bulk packaging > 3000L or 3000kg) which is a Tier 2 HSSM.

⁵ This figure does not include Tier 1 Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation) or Tier 1 Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation) or Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation). Data is unavailable on the number of these shipments.

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

In addition to the SAIs published by TSA, PL 110-53 sets up technology considerations TSA needs to factor into its hazmat truck tracking program. Congress directed TSA to factor in the results of the FMCSA’s Hazardous Materials Safety and Security Technology Field Operational Test (refer to Section 4.1) and TSA’s Hazmat Truck Security Pilot program (refer to Section 4.5). PL 110-53 includes language related to the desired capability of “smart truck” technology that Tier 1 HSSM carriers should deploy. “Smart truck” technology devices should:

- have the ability to resist tampering and disabling;
- the capability to collect, display, and store information regarding the movement of shipments of security-sensitive materials by commercial motor vehicles; and
- allow the installation by a motor carrier of concealed electronic devices on commercial motor vehicles that can be activated by law enforcement authorities to disable the vehicle or alert emergency response resources to locate and recover security-sensitive materials in the event of loss or theft of such materials.

To satisfy TSA Tier 1 HSSM and PL 110-53 requirements, the following “smart truck” devices must be deployed by Tier 1 HSSM carriers.

- GPS receiver
- Wireless modem (cellular or satellite connection)
- On-board (or handheld) computer (with wireless connection)
- Vehicle immobilization devices (with driver authentication capabilities)
- Untethered trailer tracking devices
- Driver panic button

“Smart truck” devices deployed by Tier 1 HSSM carriers must meet Transportation Security Center performance specifications. Most Tier 1 HSSM carriers will purchase a product/service package from Truck Tracking Vendors such as Qualcomm or Safefreight in which the truck tracking vendor will supply the “smart truck” hardware that carriers will install on their vehicles. In addition, the truck tracking vendor will provide fleet monitoring services to the carrier. Tier 1 HSSM carriers will need to purchase “smart truck” products/services from truck tracking vendors that are Transportation Security Center certified.

Section 4.1 described the results of the FMCSA’s Hazardous Materials Safety and Security Technology Field Operational Test. Lessons learned from the FMCSA study point out that regulations – needed to promote technology deployment – will actually generate positive ROI for hazmat carriers and will generate a huge public benefit.

- Regulations have to supply the market “push” needed to support technology deployment and data reporting – both critical to a functioning PSRC.
- Almost any combination of smart truck technology can be easily and reasonably justified from a B/C perspective.

- o The cost of technology deployment/operation is low ~\$1500/truck/year (§4.1.4).
- o Wireless communications plus GPS generates overwhelmingly positive ROI due to operational efficiency gains - \$6,000-\$10,000/truck/year depending on load type (§4.1.3).
- o FOT citation - If all the hazmat carriers in the country fully deployed "smart truck" technology it would require a one-time investment of \$543 million. But, carrier profitability would rise by \$1.7 billion/year.
- Security benefits are huge arguing for wide-spread deployment of "smart truck" technology by hazmat carriers. For example, security benefits exceeding **\$5 billion** will be captured if trucks carrying bulk chemicals were equipped with GPS, wireless modems, panic alerts and remote disabling (§4.1.8).
- Estimated security benefits argue for regulations that require smart truck technology deployment by 1). bulk fuel carriers; 2). bulk chemical carriers; and 3). truckload explosive carriers (§4.1.8). LTL high-hazard carriers are also a possibility.

6.4.1.4 Shippers, carriers and consignees of Tier 1 HSSM shipments must register with the Transportation Security Center.

As noted in the introduction to this section, data is the raw product of a truck tracking center. Without it, a truck tracking center cannot function. A truck tracking center needs access to current corporate data from hazmat shippers, carriers and consignees. For shippers, a truck tracking center needs data on shipping locations, persons authorized to act on behalf of the shipper, and the types of materials that will be shipped offsite. For carriers, a truck tracking center needs data on drivers, vehicles, permits, "smart truck" technology deployments, and relationships with shippers and truck tracking vendors. For consignees, a truck tracking center needs information on receiving facilities and facility contacts.

A registration process is the most efficient means to gather and organize this data for access by a truck tracking center and by shippers/carriers as they carry out hazmat shipment transactions.

The regulations will require Tier 1 HSSM shippers and carriers to complete registration with the Transportation Security Center.

6.4.1.5 The shipper or carrier of a Tier 1 HSSM shipment must file an electronic manifest with the Transportation Security Center before the regulated shipment may leave a shipper's facility.

An electronic manifest includes data critical to the functioning of a truck tracking center. It lists the materials (type, quantity) that are in the shipment as well as information on the shipper, the carrier, and the consignee. The electronic manifest initiates the shipment business process. The electronic manifest has to be completed before custody of the shipment can shift from the shipper to the carrier, and before the shipment may leave the shipper's facility.

Electronic manifest transaction events – such as application of digital signatures – are events that a truck tracking center will receive and process to signal the initiation of a new hazmat shipment. An electronic manifest has to be submitted prior to "gate out" in order for the truck tracking center to have visibility for that shipment. Without submission of an electronic manifest, the tracking center will not have the basic information on shipper, carrier, and load even though the vehicle is traveling over the roads.

6.4.1.6 The shipper or carrier of a Tier 1 HSSM shipment must file an electronic route plan with the Transportation Security Center before a regulated shipment may

Section 1553 of PL 110-53 will require security-sensitive hazmat carriers to develop and follow route plans. In addition TSA SAI #23 advises that Tier 1 HSSM shippers and carriers should have the ability to "define and monitor" routes and risk areas. The monitoring system should detect when a truck is off-route or

leave a shipper's facility.

nearing a risk area and send an alert to the dispatch center.

Electronic route plans are critical to a truck tracking program. Without an electronic route plan, a truck tracking system cannot track carrier route adherence and geo-fence and risk management capabilities of the system will be substantially degraded.

Like the electronic manifest, the electronic route plan must be submitted prior to "gate out" so that the truck tracking center can match the vehicle's location with its planned route.

Filing an electronic manifest with the Transportation Security Center should also trigger messaging that meets the requirements of SAI #17 – i.e. an email notice to the consignee from the consignor that a shipment is en-route and the estimated time of arrival. Upon delivery, a digital signature on the electronic manifest will trigger an email back to the consignor that the shipment was received and that the shipment was delivered in full.

6.4.1.7 Carriers of Tier 1 HSSM shipments must use the services of a fleet tracking vendor that has Transportation Security Center compliant systems and service offerings.

Section 3.1 explained that "smart truck" technology, a core technology component of a hazmat tracking system, is inexpensive and available from numerous truck tracking vendors. Section 3.1 highlighted products/services available from several truck tracking vendors.

Truck tracking vendors will be required to modify their "smart truck" product offerings to meet TSA's Tier 1 HSSM requirements and the Transportation Security Center's need for a complete set of data that it needs to operate a fully functioning truck tracking system. In addition, truck tracking vendors will be required to modify their data reporting systems to feed data to the TSC (on behalf of Tier 1 HSSM carriers) in a format that supports its needs.

6.4.1.8 A carrier's fleet tracking vendor must report the location of a carrier's vehicle hauling a Tier 1 HSSM shipment to the Transportation Security Center in a manner and at a polling frequency specified by the Transportation Security Center.

Section 3.1 described how carriers use the services of truck tracking vendors to manage their truck fleets. A GPS receiver on a carrier's truck is used to pinpoint the exact physical location of the truck using signals from GPS satellites. The position of the truck is transmitted to a truck tracking vendor via the truck's wireless modem over a wireless communications network. The truck tracking vendor will report the vehicle's location to the Transportation Security Center on a real-time basis.

SAI #23 specifies that tractor position reporting frequency should not exceed 15 minutes. The regulations will establish 15 minutes as a maximum reporting frequency for carriers hauling Tier 1 HSSMs. Location reporting must take place between "gate out" and "gate in". The Transportation Security Center may require carriers to report position more frequently for a vehicle if that vehicle's risk score warrants closer tracking.

6.4.1.9 The truck tracking vendor must report certain alerts and messages from installed smart truck devices on the carrier's vehicle to the Transportation Security Center in a manner specified by the Transportation Security Center.

Truck tracking vendors will receive data and messages from "smart truck" devices on carriers' vehicles. Truck tracking vendors are required to directly relay that information to the Transportation Security Center. This includes the following:

- vehicle location (tractor);
- driver panic alerts;
- unexpected trailer disconnect;
- unexpected trailer unloading;
- equipment tampering; and

- trailer location (after unexpected disconnect).

The truck tracking vendor must build to an XML interface published by the Transportation Security Center, and submit data in a form approved by the Transportation Security Center.

6.4.1.10 Shippers and carriers of Tier 1 HSSM shipments must respond to inquiries and alerts issued by the Transportation Security Center.

The Transportation Security Center will make inquiries when it receives alerts or information that raise concerns about a shipment. For example, a Security Specialist from the Transportation Security Center will call the carrier's hazmat contact if a carrier's truck is traveling off-route to determine if there is a "problem" with the off-route shipment. The carrier will have an obligation to act to resolve the issue and to report back to the Transportation Security Center.

SAI #14 describes special requirements HSSM carriers need to meet when DHS issues an alert that DHS Threat Conditions are red.

- **Security Action Item #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.

Under certain circumstances, TSA will declare a transportation security incident. This may then lead to a decision by TSA and/or state action agencies that a moving truck needs to be immobilized. This decision will be relayed to the truck tracking vendor, and the truck tracking vendor will be required to send a signal to the carrier's on-board immobilization systems to initiate immobilization.

6.4.1.11 A carrier and the Transportation Security Center must have the ability to communicate with a driver hauling a Tier 1 HSSM shipment.

SAI #10 requires Tier 1 and Tier 2 HSSM carriers to implement a communications plan that provides for communications between the carrier's hazmat contact and the driver.

- **Security Action Item #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.

6.4.1.12 A carrier must provide drivers of Tier 1 HSSM shipments the ability to send a panic alert both in and out of the cab.

SAI #22 requires the use of driver panic buttons.

- **Security Action Item #22. Panic Button Capability** – 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.

6.4.1.13 A shipper may not release a Tier 1 HSSM shipment to a driver that does not have a CDL with a hazmat extension or to a carrier that does not possess a FMCSA (or state-issued) hazmat safety

To meet the requirements of SAIs #5 and #17, Tier 1 HSSM shippers are prohibited from releasing a Tier 1 HSSM to a carrier that does not have a FMCSA hazmat safety permit or to a driver that does not have a commercial driver's license with a hazmat extension.

permit.

- **Security Action Item #17.** 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**.
- **Security Action Item #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.

6.4.1.14 Shippers must pay a homeland security fee for each Tier 1 HSSM shipment as well as other regulatory fees established by the state.

The Transportation Security Center will be a for-profit entity. It will generate revenue from shipment tracking transaction fees. The Transportation Security Center will track Tier 1 HSSM shipments from “gate out” to “gate in” in exchange for a homeland security fee paid by the HSSM **shipper**. This revenue model is based on the transaction fee model developed by EPA for hazardous waste e-manifest processing transactions.

6.4.2 Hazardous waste electronic manifest

Section 2.6 describes EPA’s attempt to establish a hazardous waste e-manifest program. Beginning in 2005, EPA began to issue a series of rules to pave the way for a national hazardous waste e-manifest program. On March 4, 2005 EPA published a rule in the *Federal Register* that established a uniform national manifest form. Under the old rule, States were allowed to add additional data fields to the standard manifest form. EPA’s rule eliminates that option for states. Since September 4, 2006, all jurisdictions use the exact same form.

EPA requires states to use the same hazardous waste manifest form.

On October 13, 2005 EPA published the Cross Media Environmental Reporting Rule (CROMERR 40 CFR Part 3) in the *Federal Register*. CROMERR provides a uniform, technology-neutral framework for electronic reporting across all EPA programs; allows EPA programs to offer electronic reporting as they become ready (without any additional rule-making beyond CROMERR); provides states with a streamlined process – together with a uniform set of criteria – for approval of their electronic reporting implementations for all their EPA-authorized programs; and ensures that electronic reporting under EPA and EPA-authorized state programs does not compromise the enforceability of environmental programs. Specifically, CROMERR establishes the following electronic reporting (ER) provisions:

EPA’s Cross Media Environmental Reporting Rule defines the systems infrastructure for e-manifest reporting systems.

- modified existing requirements in the Code of Federal Regulations (CFR) to remove any obstacles to ER and allow regulated entities to submit any report electronically, but only after EPA announces that ER is available for the specific report;
- required submission of electronic reports to EPA’s Central Data Exchange (CDX) or to another designated EPA system;
- required validation of electronic signatures on reports submitted to EPA through CDX (or another designated EPA system) and ensured that valid electronic signatures have the same legal force as their “wet-ink” counterparts; and
- set forth requirements that EPA-authorized programs must satisfy when implementing ER, and provided a streamlined process for these programs to get EPA approval of their ER implementations.

CROMERR is an EPA agency-wide rule that establishes electronic reporting standards for all EPA programs including standards for digital signatures, data integrity, and identity

authentication. EPA's future hazardous waste e-manifest rule will incorporate the requirements of CROMERR by reference.

As an Agency-wide rule, CROMERR is important because: 1). it sets the design/operating standards that a hazardous waste e-manifest system must meet; 2). it establishes e-manifest requirements for state authorized programs; and 3). it establishes the foundation for EPA's upcoming hazardous waste e-manifest rule. CROMERR establishes the infrastructure for EPA's hazardous waste e-manifest program.

In 2004, EPA began to explore models for building a centralized hazardous waste e-manifest processing center using a public/private development approach. EPA entered into discussions with the General Services Administration (GSA), which managed the E-Gov Act Share-in-Savings program, on a possible procurement action that might have enabled the centralized e-manifest system to be developed and operated for EPA by an information technology (IT) vendor under a "Share-in-Savings" (SiS) type contract.

EPA tried to use GSA's Share-In-Savings contract mechanism to enter into a contract with a private company to build and operate its e-manifest system.

The SiS IT contracting mechanism was authorized under the E-Gov Act of 2002 on a provisional basis as an innovative tool for Federal agencies to develop new IT systems with little direct Federal investment. The premise of the SiS contracting approach was that the IT vendor awarded an SiS contract would build the IT system at the vendor's initial expense, and then recover its costs and profit from the cost savings or enhanced revenue that results to the sponsoring agency from the new IT system. With this approach, for example, the successful e-manifest IT contractor would have incurred the initial financial risk and outlay to build the centralized e-manifest system to meet EPA's performance objectives, and then would have recovered its costs and earned its agreed profit from the revenue stream generated by the service fees (e-manifest transaction fees) paid by the users.

The GSA SiS contract program was not reauthorized by Congress leaving EPA without a path forward for implementing its e-manifest program.

In 2006, EPA reaffirmed its intent to build a national e-manifest processing center and published its vision for the system.

On April 18, 2006 EPA issued a *Federal Register* notice stating the Agency's intent to move forward with its e-manifest rule and its interest in building a national hazardous waste e-manifest processing center. EPA explained that it was considering a model in which a private developer would build and operate the e-manifest system. The system would be connected to EPA's Centralized Data Exchange (CDX) and would be built to meet EPA CROMERR requirements. Data would flow into CDX as e-manifest transactions take place. The private developer running the national processing center would collect e-manifest transaction fees in exchange for incurring the cost of building and operating the national e-manifest system. EPA's Public Notice set the stage for a push to obtain GSA share-in-savings type authority via legislation.

In 2006 EPA sought legislative authority to enter into a SiS-type contract with a private party. EPA's legislative initiative was unsuccessful. However, EPA launched a new legislative initiative in 2008 to receive Congressional authority for SiS-type contract authority.

Eventually, EPA will likely issue a simple rule to implement its hazardous waste e-manifest program. It will allow states and hazardous waste trading partners to use e-manifests instead of paper manifests provided that they process their manifests through EPA's national hazardous waste e-manifest processing center. The processing center will be built to be CROMERR-compliant and will be connected as a node to EPA's Central Data Exchange.

The regulatory elements listed below are designed to support implementation of EPA's hazardous waste electronic manifest program and to support establishment of a national hazardous waste e-manifest processing center.

6.4.2.1 Waste generators, transporters, and TSDFs may use electronic manifests instead of paper manifests.

Regulations will permit waste generators, transporters, and owner/operators of hazardous waste TSDFs (treatment, storage, disposal facilities) to use electronic manifests instead of paper manifests.

6.4.2.2 Hazardous waste shipments originating or ending in Kentucky are subject to Kentucky's hazardous waste electronic manifest regulations.

Hazardous waste shipments involve three parties: 1). waste generators; 2). waste transporters; and 3). waste management firms (TSDFs). Shipments from generators located in Kentucky will be subject to Kentucky's hazardous waste e-manifest regulations. This will be the case even if the shipments are to waste management facilities located out of the state. Also, shipments from out-of-state waste generators to waste management facilities located in Kentucky will also be subject to Kentucky's regulations. Ontario's Regulation 347 applied a similar regulatory construct (refer to Section 4.7).

6.4.2.3 Waste generators, transporters, and TSDFs must register with the Transportation Security Center.

A registration process is necessary to populate the system with the raw data it needs to support an electronic manifest program. Regulations will require generators, transporters, and waste management facilities to provide the data needed via an on-line registration process. Again, Ontario's regulatory program and its Hazardous Waste Information Network (HWIN) provide the example of how the registration program would work (refer to Section 4.7).

6.4.2.4 A waste generator may not release a hazardous waste shipment to a driver that does not have a CDL with a hazmat extension.

Section 2.1 explained that hazardous wastes are, in fact, a small subset of the much larger universe of hazardous materials (hazmat). TSA regulations require each hazmat driver to obtain a commercial driver's licenses with a hazmat extension (refer to Section 2.2.2). A waste generator will be required to verify that the driver has the appropriate credentials (CDL with hazmat extension) before releasing custody of the waste shipment to the driver.

6.4.2.5 Hazardous waste electronic manifest transactions must be processed through the Transportation Security Center. The manifest must be processed before "gate out".

Regulations will require hazardous waste electronic manifests to be processed through the Transportation Security Center. The Transportation Security Center will have national service scope and will process e-manifests from any state.

An electronic manifest includes data critical to the functioning of an e-manifest processing center. It lists the wastes (type, quantity) that are in the shipment as well as information on the shipper, the transporter, and the waste management facility. The electronic manifest initiates the e-manifest business process. The electronic manifest has to be completed before custody of the waste shipment can shift from the generator to the transporter, and before the transporter may leave the shipper's facility.

Electronic manifest transaction events – such as application of digital signatures – are events that the e-manifest processing center will receive and process to signal the initiation of a new hazardous waste shipment. An electronic manifest has to be submitted prior to "gate out" in order for the e-manifest processing center to have visibility for that shipment. Without submission of an electronic manifest, the tracking center will not have the basic information on shipper, carrier, and load even though the vehicle is traveling over the roads. And without this visibility, there will be no chain-of-custody control over the waste shipment.

6.4.2.6 Waste generators and TSDFs must pay regulatory fees established by EPA or the state.

The regulations will require waste generators and waste management firms to pay regulatory fees. Many states currently require payment of regulatory fees related to their hazardous waste programs. Kentucky, for example, collects a variety of fees from hazardous waste generators (refer to Section 6.5.1.2).

Ontario's Regulation 347 established regulatory fees for hazardous

waste generators: 1). CAD\$50 base fee payable annually; 2). CAD\$5 for each manifest used to ship waste off-site; and 3). CAD\$10/tonne of hazardous waste generated. Ontario generates about CAD\$9 million/year in regulatory fees.

At a minimum, regulations will establish a manifest transaction fee. EPA estimates that each e-manifest transaction will save about \$75. Waste transporters and waste management firms together capture about two-thirds of available e-manifest cost savings – about \$50/manifest transaction. Many waste transporters are captive transporters – ie. they are owned by waste management firms and haul exclusively for their parent companies. When viewed in this light, the waste management firms will be the largest beneficiaries of EPA's e-manifest program.

	Unit Cost Savings % Distribution	Unit Cost Savings \$ Distribution
Waste Generators	22%	\$16.67
Waste Management Firms	47%	\$34.96
Waste Transporters	20%	\$14.99
State Agencies	11%	\$8.20
EPA	0%	\$0.00
Total	100%	\$74.82

E-manifest regulatory fees will be shared by generators and waste management firms given that both parties benefit.

E-manifest regulatory fees will be established that are much lower than the cost savings estimated by EPA.

6.4.2.7 Use of electronic manifests is voluntary however parties to the manifest transaction will pay higher regulatory fees for paper manifest processing.

The regulations will not require mandatory use of electronic manifests. However, the regulatory goal will be near 100% e-manifest use by the waste trading partners.

The e-manifest experience in Ontario demonstrated that waste trading partners will not transition to e-manifests without a regulatory/financial incentive. This was true even though e-manifests deliver cost savings of about \$75/manifest transaction (refer to Section 2.6).

As noted in the previous section, regulations will establish a fee program for manifest processing. The fee for processing a paper manifest will be set higher than the fee for an e-manifest to encourage e-manifest use. The e-manifest transaction processing fee will be shared by waste generators and waste management firms, the major beneficiaries of an e-manifest program. However, hazardous waste e-manifest regulatory fee allocation will reflect the relative e-manifest cost savings of the parties. The waste management firms – the primary financial beneficiary of an e-manifest program – will likely assume the larger portion of the incremental cost of using paper manifests.

6.4.2.8 A waste transporter may serve as an "offeror" and sign a manifest on behalf of the waste generator.

On September 4, 2006 EPA published a rule that established a fundamental shift in the relationship between waste generators and waste transporters. The rule discusses the new role of "offeror" in the EPA hazardous waste manifest process. The status of an offeror is well developed under DOT's hazardous materials regulations. Under DOT rules, an offeror is any person involved with performing certain "pre-transportation" functions that occur before hazardous materials are transported in

commerce. An offeror may prepare shipping papers on behalf of hazmat shippers and sign the shipper's certification on the DOT shipping papers. EPA has adopted DOT's concept of offeror, and will allow offerors to sign hazardous waste manifests on behalf of the waste generator.

The model regulation will recognize the role of an offeror and systems underlying the Transportation Security Center will accommodate the offeror's role in the e-manifest business process.

6.4.2.9 A waste transporter is not required to install "smart truck" devices or use a fleet tracking vendor but it is strongly encouraged (optional regulatory element)

Unlike Tier 1 HSSM carriers, waste transporters will not be required to install "smart truck" devices or use a truck tracking vendor. However, some states may want to require shipment tracking to strengthen chain-of-custody control over hazardous waste shipments. It should be noted that an on-board computer and wireless modem – basic building blocks of a truck tracking program – will directly serve the needs of a hazardous waste electronic manifest program. By deploying these devices, the waste transporter will bring computing capability and internet connectivity to the critical generator/transporter manifest transaction. The experience in Ontario shows that this will address a major implementation flaw in an e-manifest program. Refer to Section 4.7 for additional information.

6.5 Kentucky statutes and regulations

This section describes Kentucky's hazardous waste and hazmat statutes/regulations that are currently on the books. Implementing a model regulatory program will require refinements to the current set of statutes and regulations. Section 6.5.1 provides an overview of the statutes and regulations that are currently in force in Kentucky. Section 6.5.2 describes refinements that Kentucky cabinet agencies would need to seek to implement the model regulatory program.

6.5.1 Current statutes and regulations

Section 6.5.1.1 describes Kentucky's hazardous materials program. Section 6.5.1.2 describes Kentucky's hazardous waste program.

6.5.1.1 Kentucky's hazardous materials program⁶

Kentucky has adopted statutes and regulations for its hazmat program. Chapter 174 of the Kentucky revised statutes describes the legislative intent of Kentucky's hazmat regulations.

174.400 Legislative intent.

Due to the central geographical location of the Commonwealth with respect to the hazardous materials industry, and since most predictions indicate that the amount of hazardous material in transport should substantially increase in the future, it is the intent of KRS 174.405 to 174.425 to provide for the public health and safety of the citizens and to protect the environment of the Commonwealth when any hazardous material is being transported within, or, in the case of radioactive materials, within or through this state.

Effective: July 15, 1994

History: Amended 1994 Ky. Acts ch. 99, sec. 2, effective July 15, 1994. – Created 1980 Ky. Acts ch. 384, sec. 1, effective July 15, 1980.

Kentucky's current hazmat program incorporated federal rules by reference.

⁶ Kentucky Revised Statutes - <http://www.lrc.ky.gov/krs/titles.htm>
Kentucky Administrative Regulations - <http://www.lrc.ky.gov/kar/601/001/025.htm>

Kentucky's hazmat statute directs the Transportation Secretary to "adopt by reference or in entirety, the Federal Hazardous Materials Transportation Regulations, 49 C.F.R. (1978), as amended, to effectively carry out the intent of KRS 174.400 to 174.425." This means that Kentucky's hazmat regulatory program is a virtual mirror image of the federal regulatory program.

Extracts from Kentucky revised statutes dealing with hazardous materials may be found in **Appendix H**. Notable features of Kentucky's hazardous materials statute:

- The Transportation Secretary is responsible for controlling and regulating the movement of all radioactive materials and the intrastate transport of other hazardous materials transported by all carrier modes within the Commonwealth. (174.410(1) administrative regulations and agreements with other cabinets)
- The Transportation Cabinet and the Justice Cabinet shall cooperate with and assist the Environmental and Public Protection Cabinet in implementing and enforcing the transportation provisions of any state hazardous waste regulations promulgated pursuant to KRS Chapter 224. The specific nature and details of the assistance effort shall be established by a formal cooperative agreement acceptable to the cabinets, and all activities shall occur in accordance with the terms of the agreement. (174.410(3) administrative regulations and agreements with other cabinets)

6.5.1.2 Kentucky's hazardous waste program⁷

Kentucky has adopted statutes and regulations for its hazardous waste program. Chapter 224 of the Kentucky revised statutes describes the authority of the Environmental and Public Protection Cabinet (EPPC) and describes the regulatory structure of the state's hazardous waste program. (Chapter 224 Subchapter 46).

Extracts from Kentucky revised statutes dealing with hazardous waste may be found in **Appendix G**. Notable features of Kentucky's hazardous waste statutes:

- Kentucky requires hazardous waste generators to pay annual registration fees (224.46-012 Registration fee for generator of hazardous waste).
- Kentucky requires hazardous waste generators to pay waste generation fees (224.46-580(7) hazardous waste assessment).
- The cabinet shall promulgate regulations establishing standards applicable to transporters of hazardous waste regarding record keeping, notification and compliance with the manifest system. The Transportation Cabinet and the Justice Cabinet shall cooperate with and assist the cabinet in implementing and enforcing the transportation provisions of any state hazardous waste regulations promulgated pursuant to this chapter. The specific nature and details of the assistance effort shall be established by a formal cooperative agreement acceptable to the cabinets. (224.46-560 Standards relating to transporters -- Agency cooperation)
- The Cabinet is authorized to deposit fees into the hazardous waste management fund. The fund balance will not exceed \$6 million or fall below \$3 million. (224.46-580(13) Hazardous waste management fund)

224.46-580(15) Upon request of the secretary, moneys accumulated in the hazardous waste management fund shall be released in amounts necessary to accomplish the performance of the duties imposed by subsection (3) of this section.

- The cabinet shall require the use of a manifest system for the orderly tracking of hazardous wastes from the generation site to the site of treatment, storage, and disposal except for coal mining wastes pursuant to KRS 224.50-760(1)(c). The system shall, at a minimum, require the designation of the generator, each transporter, the disposal facility, and the type and quantity of waste involved. The

DOT has delegated responsibility for the hazmat program to Kentucky. The Transportation Cabinet and the Justice and Public Safety Cabinet are responsible for the program.

Kentucky's hazardous waste program includes a set of regulatory fees on waste generators. Fees flow into the hazardous waste management fund.

EPA has delegated authority for the hazardous waste program to Kentucky. The Environmental and Public Protection Cabinet has responsibility for the program.

⁷ Kentucky Revised Statutes - <http://www.lrc.ky.gov/krs/titles.htm>
Kentucky Administrative Regulations – Title 401 <http://www.lrc.ky.gov/kar/TITLE401.HTM>

cabinet may establish additional criteria to accommodate the manifest system to internal record keeping and to facilitate the monitoring of hazardous waste activity within the Commonwealth. (224.46-570 Manifest system)

Kentucky is authorized by EPA to operate the hazardous waste program in Kentucky in lieu of EPA. State authorization is a rulemaking process through which EPA delegates the primary responsibility of implementing the RCRA hazardous waste program to individual states in lieu of EPA. This process ensures national consistency and minimum standards while providing flexibility to states in implementing rules.

State RCRA programs must always be at least **as stringent** as the federal requirements, but states can adopt **more stringent** requirements as well. Refer to EPA URL on state authorization of hazardous waste programs.

<http://www.epa.gov/epaoswer/hazwaste/state/index.htm>

From time to time, EPA will revise its regulations. As states must have statutes/regulations at least as stringent as EPA's, there is a constant modification of state statutes and state regulatory provisions. For example, in 2005, EPA promulgated a major rule that will establish a uniform national manifest for hazardous waste shipments. As part of that rule, EPA published guidance for authorized states to advise them how they would need to revise their regulations/statutes to ensure consistency with the EPA uniform manifest rule.

6.5.2 Recommended statutory refinements – Tier 1 HSSM tracking

Section 6.4.1 described the regulatory elements that should underlie a Tier 1 HSSM truck tracking program. They are listed below.

- Shipments of TSA-designated Tier 1 highway security-sensitive shipments (HSSMs) are "regulated shipments".
- Tier 1 HSSM shipments traveling over Kentucky's roads must meet Kentucky's hazmat shipment security requirements.
- Carriers of Tier 1 HSSM shipments must install smart truck devices that are Transportation Security Center compliant.
- Shippers and carriers of Tier 1 HSSM must register with the Transportation Security Center.
- The shipper or carrier of a Tier 1 HSSM shipment must file an electronic manifest with the Transportation Security Center before the regulated shipment may leave a shipper's facility.
- The shipper or carrier of a Tier 1 HSSM shipment must file an electronic route plan with the Transportation Security Center before a regulated shipment may leave a shipper's facility.
- Carriers of Tier 1 HSSM shipments must use the services of a fleet tracking vendor that has Transportation Security Center compliant systems and service offerings.
- A carrier's fleet tracking vendor must report the location of a carrier's vehicle hauling a regulated shipment to the Transportation Security Center in a manner and at a polling frequency specified by the Transportation Security Center.
- The truck tracking vendor must report certain alerts and messages from installed smart truck devices on the carrier's vehicle to the Transportation Security Center in a manner specified by the Transportation Security Center.
- Shippers and carriers of Tier 1 HSSM shipments must respond to inquiries and alerts issued by the Transportation Security Center.
- A carrier and the Transportation Security Center must have the ability to verbally communicate with a driver hauling a regulated shipment.
- A carrier must provide drivers of Tier 1 HSSM shipments the ability to send a panic alert both in and out of the cab.
- A Tier 1 HSSM shipper may not release a regulated shipment to a driver that does not have a CDL with a hazmat extension or a FMCSA or state-issued hazmat safety permit.

Regulations will be a key driver for establishment of a Tier 1 HSSM truck tracking program.

- Shippers must pay a homeland security fee for each Tier 1 HSSM shipment as well as other regulatory fees established by the state.

Kentucky's statutory program would need to be refined to support implementation of a program incorporating these regulatory elements. Specifically, the following refinements would be needed.

1. Broaden Section 174.400 which describes the legislative intent of Kentucky's hazmat program slightly to add public security to public health and safety as the driving forces behind Kentucky's hazmat program.
2. Revise Sections 174.410 and 174.415 to reflect the role of the Kentucky Office of Homeland Security in hazmat supply chain security issues and to reinforce the primary role of the Kentucky Transportation Cabinet in hazmat regulatory and enforcement matters.
3. Add a new section to provide the Secretary of the Transportation Cabinet the authority to commit the Commonwealth to membership in the Alliance for Uniform Hazmat Transportation Procedures if the Secretary determines that membership is advantageous to the Commonwealth.
4. Add a new section that allows the Secretary of the Transportation Cabinet to implement regulations to institute regulatory fees on hazmat carriers consistent with membership in the Alliance for Uniform Hazmat Transportation Procedures and the cost of hazmat services provided by Commonwealth agencies. Add a provision that allows the Secretary of the Transportation Cabinet to implement a homeland security fee for high-risk hazmat shipments on Kentucky's roads.
5. Add a new section authorizing the Secretary of the Transportation Cabinet to depart from Kentucky's current regulatory approach of incorporating by reference federal hazmat regulations. Authorize the Secretary to implement regulations that enhance security of high-risk hazmat shipments on Kentucky's roads.

Kentucky's statutes need refinement to pave the way for implementing regulations that will drive a Tier 1 HSSM truck tracking program.

6.5.3 Recommended statutory refinements - hazardous waste electronic manifest

Section 6.4.2 described the regulatory elements that should underlie a hazardous waste e-manifest program. They are listed below.

- Waste generators, transporters, and TSDFs may use electronic manifests instead of paper manifests.
- Hazardous waste shipments originating or ending in Kentucky are subject to Kentucky's hazardous waste electronic manifest regulations.
- Waste generators, transporters, and TSDFs must register with the Transportation Security Center.
- A waste generator may not release a hazardous waste shipment to a driver that does not have a CDL with a hazmat extension.
- Hazardous waste electronic manifest transactions must be processed through the Transportation Security Center.
- Use of electronic manifests is voluntary however parties to the manifest transaction will pay higher regulatory fees for paper manifest processing.
- A waste transporter may serve as an "offeror" and sign a manifest on behalf of the waste generator.
- Waste generators and TSDFs must pay regulatory fees established by EPA or the state.
- A waste transporter is not required to install smart truck devices or use a fleet tracking vendor but it is strongly encouraged (optional regulatory element).

Regulations will be a key driver for establishment of a hazardous waste electronic manifest program.

Kentucky's statutory program would need to be refined to support implementation of a program incorporating these regulatory elements. Specifically, the following refinements would be needed.

1. Revise Section 224.46 to refine regulatory fee schedule.
2. Revise Section 224.46 – 570 to authorize the use of hazardous waste electronic manifests for hazardous waste shipments originating or terminating in Kentucky. (Note: may only require a regulatory amendment.)
3. Revise 224.46 – 580 to authorize the Secretary of the Environmental and Public Protection Cabinet to use the hazardous waste management fund to collect regulatory fees and to disburse funds to support implementation of a hazardous waste electronic manifest program.

Kentucky's statutes need refinement to pave the way for implementing regulations that will drive a hazardous waste e-manifest program.



7.0 The North American Transportation Security Center

The North American Transportation Security Center will serve as the implementing tool for regulations that will require:

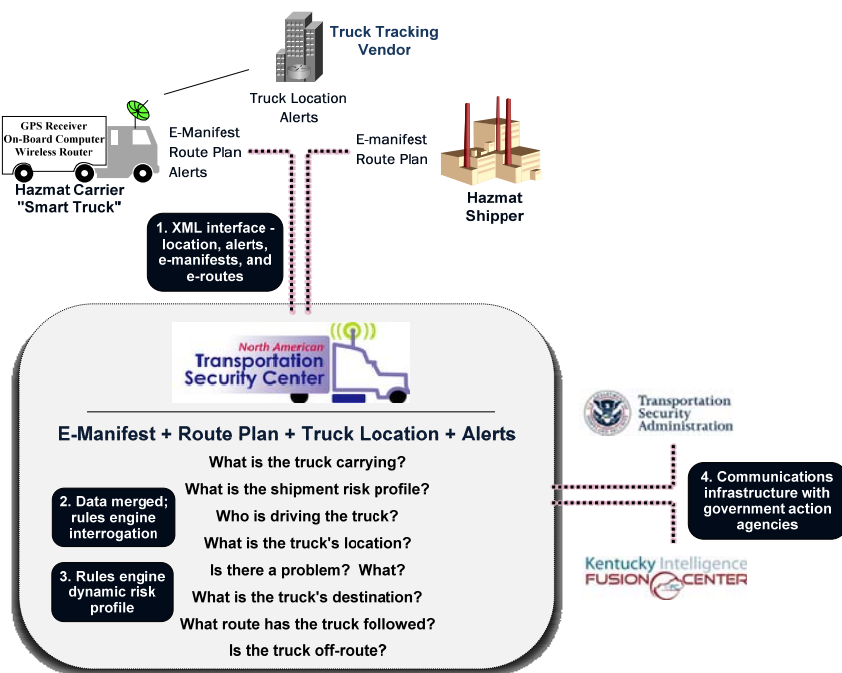
- Tier 1 HSSM carriers to install “smart truck” technology on their vehicles;
- shippers and carriers to send electronic manifests and electronic route plans to the Transportation Security Center;
- carriers to report vehicle location and alerts to the Transportation Security Center (real-time XML data feed); and
- companies to pay hazmat regulatory fees.

The Transportation Security Center will also serve as the implementing tool for a model hazardous waste electronic manifest regulatory program.

Figure 7.a illustrates the hazmat tracking features of the Transportation Security Center. The Transportation Security Center will use the basic building blocks described in Section 4.5.2. A “smart truck” equipped with an on-board computer, GPS receiver, and a wireless modem will use an internet connection (satellite or cellular) to interact with the Transportation Security Center and a commercial fleet tracking data center. E-manifest transactions between the carrier and the Transportation Security Center will provide the Transportation Security Center with information on the types and quantities of materials the transporter is hauling as well as shipment status (i.e. awaiting pickup, in transit, etc.). Data from the carrier’s fleet tracking data center will provide the Transportation Security Center the carrier’s exact location at all times. The shipper and/or carrier will also submit route plans. Alerts from the shipper or carrier will be generated when different events occur. The Transportation Security Center will merge e-manifest, vehicle location, route and alert data to provide government officials real-time visibility into the security status of hazmat shipments. In the event of a security incident, the Transportation Security Center will interact with State and Federal operations centers Kentucky’s Intelligence Fusion Center is the state action agency in the Commonwealth.

The North American Transportation Security Center will be the implementing tool for hazmat shipment tracking regulations.

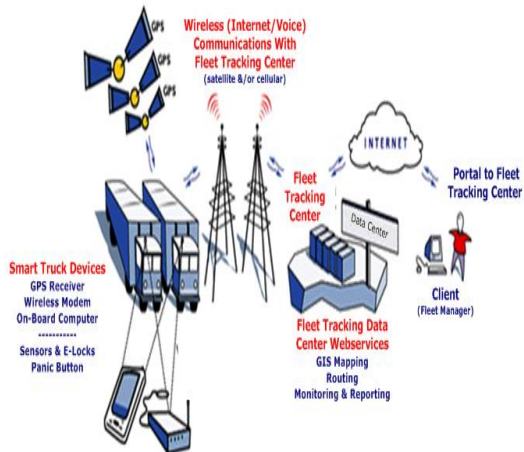
Figure 7.a Hazmat tracking at the North American Transportation Security Center.



The building blocks of a hazmat truck tracking center are:

1. an XML –based communications interface;
2. an operations center that processes data into actionable intelligence;
3. a business rules engine for dynamic risk profiling of hazmat shipments; and
4. a communications infrastructure for collaboration with action agencies.

<p>7.1 The North American Transportation Security Center will operate as a for-profit business; will use the EPA-inspired transaction fee revenue model.</p>	<p>EPA's "share-in-savings" business model calls for a private company to build and operate an e-manifest processing center. The company will collect a transaction fee for each hazardous waste electronic manifest it processes. A business model based on transaction fee revenues will work equally well for hazmat shipments, and can be extended to a for-profit model for a hazmat truck tracking center. In the hazmat case, the transaction would begin at "gate out" and would end at "gate in". The fee paid would be for tracking services from "gate out" to "gate in".</p>
<p>7.2 The North American Transportation Security Center will serve as TSA's hazmat truck tracking center.</p>	<p>PL 110-53 requires TSA to develop a HSSM truck tracking program. The North American Transportation Security Center will meet TSA's need for a truck tracking center.</p>
<p>7.3 The North American Transportation Security Center will serve as EPA's hazardous waste electronic manifest processing center.</p>	<p>EPA is committed to the establishment of a hazardous waste electronic manifest processing center. The North American Transportation Security Center will meet EPA's need for an e-manifest processing center.</p>
<p>7.4 The hazmat truck tracking services offered by the North American Transportation Security Center will operate under the FedTrak.com™ brand name.</p>	<p>The hazmat truck tracking services offered by the Transportation Security Center will operate under the brand name, FedTrak.com™. FedTrak.com™ will serve the needs of hazmat shippers and carriers. In addition, FedTrak.com™ will interface with state and federal action agencies to serve their needs for high-risk hazmat shipment tracking.</p>
<p>7.5 FedTrak.com™ will provide truck tracking services for shipments of TSA-designated Tier 1 Highway Security-Sensitive Materials.</p>	<p>FedTrak.com™ will provide truck tracking services for Tier 1 HSSMs. Refer to Section 6.4.1.1 for a discussion of the rationale for tracking Tier 1 HSSMs. TSA defines the following hazardous materials as Tier 1 HSSMs.</p> <ul style="list-style-type: none"> • Division 1.1, Division 1.2, Division 1.3 - Explosives • Division 2.2 - Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation) • Division 2.3 - Toxic (Poison) Gas • Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation) • Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation) • Class 7 Radioactive Materials • Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation) • Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules. <p>There are less than 2 million Tier 1 HSSM shipments per year in the U.S. This represents well less than 1% of all hazmat shipments.</p>
<p>7.6 Tier 1 HSSM carriers must use the services of a FedTrak.com™ certified hazmat truck tracking vendor.</p>	<p>As illustrated in the figure in the left column, a typical "smart truck" technology deployment connects truck-mounted smart truck devices to a truck tracking vendor's fleet tracking data center via a wireless modem on the truck. This set-up allows carrier fleet managers to track the location and status of the trucks in their fleets on a real-</p>



time basis via an internet connection. Fleet managers use GIS tools (mapping, routing, reporting) and in-cab messaging systems to monitor and manage fleet activity.

The cost of deploying and operating “smart truck” technology systems is low and the market for smart truck technology is well established (Section 3.1.2). Hazmat carriers use the services of commercial truck tracking vendors such as Qualcomm and Safefreight Technology (see Figure 3.1.b).

Many trucking companies have already installed smart truck fleet tracking systems. Over the past 15 years, for example, Qualcomm has installed its commercial communications and vehicle tracking technology on more than 500,000 commercial vehicles. According to the company, Qualcomm customers include more than 1,500 trucking companies and 34 of the top 35 truckload fleets.

The North American Transportation Security Center will not create “smart truck” technology. Instead, it will leverage the technology offered by existing commercial truck tracking vendors. The FMCSA study (Section 4.1) and the TSA Hazmat Truck Security Pilot program (Section 4.5) demonstrated the value of leveraging the product/service offerings of commercial truck tracking vendors. Truck tracking vendors have the ability to forward on vehicle location and other alerts to a hazmat truck tracking center using a real-time XML data feed.

Commercial truck tracking vendors anticipate that government regulation will dictate the deployment of “smart truck” technology in segments of the hazmat transportation market (see Section 5.1). Product development by “smart truck” technology vendors has increasingly focused on developing product security features, and product marketing has increasingly emphasized hazmat shipment security.

Truck tracking vendors will be required to fine-tune their “smart truck” product offerings to meet TSA’s Tier 1 HSSM requirements and the Transportation Security Center’s need for a complete set of data that it needs to operate a fully functioning truck tracking system (see Section 6.4.1.7). However, these modifications should be relatively minor. In addition, truck tracking vendors will be required to modify their data reporting systems to feed data to the Transportation Security Center (on behalf of Tier 1 HSSM carriers) in a format that supports the Transportation Security Center’s needs.

Under this regulatory/implementation approach, truck tracking vendors will serve as a new ‘regulatory character’ working in concert with hazmat carriers and the North American Transportation Security Center.

7.7 Tier 1 HSSM carriers must install FedTrak.com™ compliant “smart truck” technology devices on their vehicles.

Tier 1 HSSM carriers will be required to install the following “smart truck” devices on their vehicles.

- GPS receiver
- Wireless modem (cellular or satellite connection)
- On-board (or handheld) computer (with wireless connection)
- Vehicle immobilization devices (with driver authentication capabilities)
- Untethered trailer tracking devices
- Driver panic button

Section 6.4.1.3 discussed the regulatory rationale for the inclusion

of these devices as part of the “smart truck” technology suite for Tier 1 HSSM vehicles.

“Smart truck” devices deployed by Tier 1 HSSM carriers must meet Transportation Security Center performance specifications. Most Tier 1 HSSM carriers will purchase a product/service package from truck tracking vendors such as Qualcomm or Safefreight in which the truck tracking vendor will supply the “smart truck” hardware that carriers will install on their vehicles. Refer to Sections 3.1, 4.2, and 4.3 for information on commercial offerings by “smart truck” technology vendors.

7.8 Incident management will follow a defined workflow.

Figure 7.8 illustrates the workflow that CTU Security Specialists will follow when a driver panic alert is received by FedTrak.com™. The Security Specialist will contact the carrier first to determine if the alert is a “false alarm”. If so, the case is closed. However, if it is determined that the alarm is genuine, the Security Specialist will bridge a TSA Watch Officer and the state operations center into a conference call. The TSA Watch Officer has the option of declaring the shipment of “security interest” or declaring a “transportation security incident”.¹

7.9 Shippers of Tier 1 HSSMs will pay a homeland security fee for each “gate out” to “gate-in” transaction.

EPA’s “share-in-savings” business model calls for a private company to build and operate an e-manifest processing center. The company will collect a transaction fee for each hazardous waste electronic manifest it processes. A revenue model based on transaction fees will work equally well for hazmat shipments. Refer to Section 5.3.2 and Section 6.4.1.14.

FedTrak.com™ will generate revenue from shipment tracking transaction fees. FedTrak.com™ will track Tier 1 HSSM shipments from “gate out” to “gate in”. Tier 1 **HSSM shippers** will pay a homeland security (transaction) fee for shipment tracking.

7.10 The hazardous waste electronic manifest services offered by the North American Transportation Security Center will operate under the FedWaste.com™ brand name.

The hazardous waste e-manifest services offered by the Transportation Security Center will operate under the brand name, **FedWaste.com™**. FedWaste.com™ will serve the needs of hazardous waste generators, transporters, and owner/operators of waste management facilities. In addition, FedWaste.com™ will interface with state and federal action agencies to serve their needs for hazardous waste e-manifest processing.

7.11 FedWaste.com™ will be EPA CROMERR-compliant and will serve as a node on EPA’s Central Data Exchange (CDX) system.

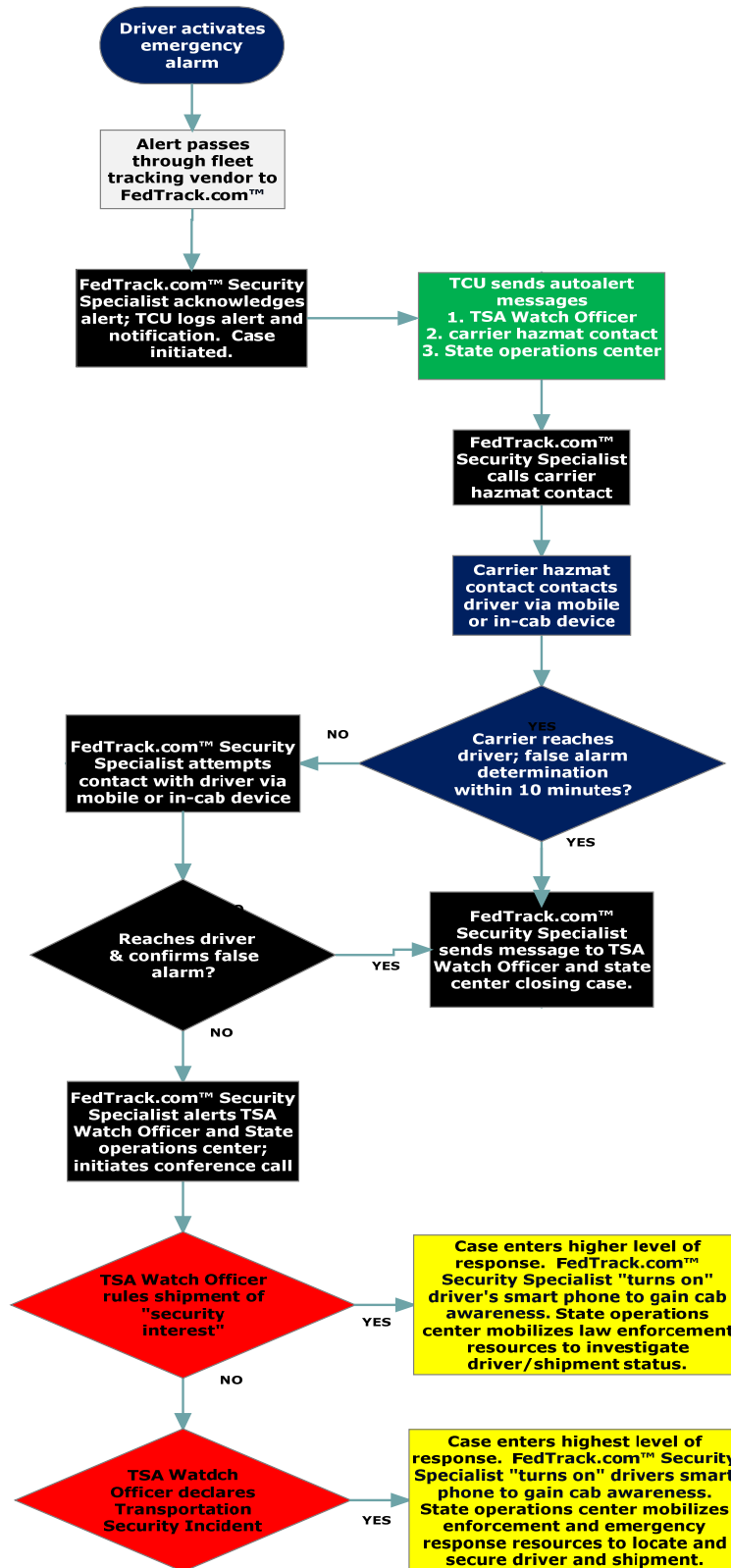
Section 2.6.3.3 described EPA’s Cross Media Environmental Reporting Rule (CROMERR). CROMERR is an EPA agency-wide rule that establishes electronic reporting standards for all EPA programs including standards for digital signatures, data integrity, and identity authentication. EPA’s future hazardous waste e-manifest rule will incorporate the requirements of CROMERR by reference.

As an Agency-wide rule, CROMERR is important to a hazardous waste e-manifest program because: 1). it sets the design/operating standards that a hazardous waste e-manifest system must meet; 2). it establishes e-manifest requirements for state authorized programs; and 3). it establishes the foundation for EPA’s upcoming hazardous waste e-manifest rule.

On April 18, 2006 EPA issued a *Federal Register* notice stating the Agency’s intent to move forward with its e-manifest rule and its

¹ A transportation security incident (TSI) is defined by TSA as a security incident resulting in significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area (46 USC 701).

Figure 7.8 FedTrak.com™ incident management workflow.



interest in building a national hazardous waste e-manifest processing center. EPA explained that it was considering a model in which a private developer would build and operate the e-manifest system. The system would be connected to EPA's Centralized Data Exchange (CDX) and would be built to meet EPA CROMERR requirements. Data would flow into CDX as e-manifest transactions take place. The private developer running the national processing center would collect e-manifest transaction fees in exchange for incurring the cost of building and operating the national e-manifest system. See Section 2.6.3.5.

FedWaste.com™ will be EPA CROMERR-compliant and will serve as a node on EPA's Central Data Exchange (CDX) system. See Section 2.6.3.5.

7.12 FedWaste.com™ will integrate the business processes of waste generators, transporters, waste firms, and regulatory agencies.

FedWaste.com™ will link the business processes of waste generators, waste haulers, waste firms and regulatory agencies. It will allow user data to flow efficiently though FedWaste.com™ to support external business processes as well as meeting internal FedWaste.com™ e-manifest business processes. Published XML interfaces will allow system users to efficiently link to the e-manifest system.

7.13 FedWaste.com™ will collect a transaction fee for processing an e-manifest on behalf of EPA or a state agency.

EPA's "share-in-savings" business model calls for a private company to build and operate an e-manifest processing center. The private company will collect a transaction fee for each hazardous waste electronic manifest it processes.

On April 18, 2006 EPA issued a *Federal Register* notice stating the Agency's intent to move forward with its e-manifest rule and its interest in building a national hazardous waste e-manifest processing center. EPA explained that it was considering a model in which a private developer would build and operate the e-manifest system. The system would be connected to EPA's Centralized Data Exchange (CDX) and would be built to meet EPA CROMERR requirements. Data would flow into CDX as e-manifest transactions take place. The private developer running the national processing center would collect e-manifest transaction fees in exchange for incurring the cost of building and operating the national e-manifest system.

On February 26, 2008, EPA published a Notice of Data Availability in the *Federal Register* that reaffirmed EPA's intent to issue an electronic manifest rule and to seek federal legislation giving it share-in-savings type authority to support implementation of a national e-manifest processing center.

FedWaste.com™ will generate revenue from hazardous waste manifest processing transaction fees. Hazardous waste generators and owner/operators of treatment, storage and disposal facilities (TSDFs) will pay a fee for each manifest processed by FedWaste.com™.

FedWaste.com™ will provide manifest processing service on behalf of EPA if EPA implements a national e-manifest regulatory program or on behalf of states if states are given the option of choosing to implement e-manifest programs.

7.14 FedWaste.com™ will provide the states a mechanism to implement regulatory fee programs and to efficiently

FedWaste.com™ will process regulatory fee payments by hazardous waste generators and TSDF owner/operators. FedWaste.com™ will serve as a regulatory fee payment portal for generators and TSDFs. Regulatory fee payments systems in

collect payments.

Ontario's HWIN system are illustrative of fee payment functionality that will be built into FedWaste.com™ (see Section 4.7 and Figure 4.7.a).

7.15 E-manifest regulatory fees will be paid by waste generators and waste firms; can be a significant revenue source for states.

EPA estimates that an e-manifest will save \$75/manifest transaction. As shown in the table below, waste transporters and waste management firms together capture about two-thirds of available e-manifest cost savings – about \$50/manifest transaction. Waste generators and state agencies capture the remainder. With about 4 million hazardous waste shipments in the U.S. each year, electronic manifests have the potential to generate savings of more than \$300 million per year.

	Unit Cost Savings % Distribution	Unit Cost Savings \$ Distribution
Waste Generators	22%	\$16.67
Waste Management Firms	47%	\$34.96
Waste Transporters	20%	\$14.99
State Agencies	11%	\$8.20
EPA	0%	\$0.00
Total	100%	\$74.82

Cash-strapped states are increasingly looking for revenue opportunities. Kentucky, like many other states, currently has regulations in place that require waste generators to pay fees based on waste generation.

Section 4.7 described how the Province of Ontario crafted a regulatory fee program to generate CAD\$10 million/year in revenue including a fee for each manifest transaction. With the inherent cost savings associated with e-manifests (e.g. \$75/transaction), there is plenty of room for a state to collect regulatory fees and still deliver a benefit to regulated companies by implementing an e-manifest program. Ontario's hazardous waste program is a good example (see Section 4.7). Even with an extremely hefty regulatory fee structure, e-manifests offer Ontario waste generators a healthy benefit/cost value proposition.

With about 200,000 manifest transactions/year, the use of e-manifests instead of paper manifests has the potential of generating US\$15 million in annual cost savings (200,000 x \$75) in Ontario. Ontario collects about CAD\$9 million/year (US\$10.2 million) in regulatory fees from waste generators. Assuming full e-manifest use, the benefit/cost ratio for an e-manifest program in Ontario is ~1.5 (B=\$15million; C=\$10.2 million). This is an impressive B/C ratio considering the heavy regulatory fee burden Ontario places on waste generators.

7.16 FedWaste.com™ will operate a paper manifest processing center in conjunction with FedWaste.com™.

On February 26, 2008, EPA published a Notice of Data Availability in the *Federal Register*. The notice asked for comment on a refinement to EPA's implementation plan for its e-manifest processing center. EPA expects e-manifest use will be voluntary and that many manifest transactions will continue to be paper based. However, EPA recognizes that a manifest database that holds data on only electronic transactions would be less valuable than one that holds both electronic and paper transactions. EPA has proposed for comment a plan to amend its manifest regulations so that the final destination facility (and only the destination facility) would mail a copy of the completed manifest form to the e-manifest system operator. The system operator would scan the form and enter manifest data from it into the national manifest database. EPA expects the final destination

facility would pay the cost of data processing for paper manifests.

This proposal will likely have a huge impact on EPA's manifest operations center. E-manifest use would be purely voluntary. Unless companies moved voluntarily to e-manifest use, most of the transactions would be paper-based making document processing the main focus of the national e-manifest processing center. EPA expects the destination facility would mail a final copy of the manifest to the system operator and pay a fee to the system operator for paper manifest processing.

FedWaste.com™ will operate a paper manifest processing center in conjunction with FedWaste.com™. The emphasis will be on high-speed forms processing. Completed forms would be posted on My FedWaste.com™. This is similar to the approach taken by Ontario in its HWIN system. Figure 4.7.b illustrates the process followed in Ontario. After paper manifest forms are scanned and the data from the forms entered into an interim database, the data and the scanned form are ported over to HWIN. The data as well as the scanned image is available to generators, transporters, and TSDFs via their MyHWIN pages.

FedWaste.com™ will use a double blind keying process to process paper manifest forms. Two different data entry operators will process each form. The results will be compared to make sure that the information corresponds. The objective is 99.9% accuracy.

7.17 Higher transaction fees for paper manifests will promote e-manifest use.

As discussed in Section 6.4.2.7, regulations will not require mandatory use of electronic manifests. However, the regulatory goal will be near 100% e-manifest use by the waste trading partners.

The e-manifest experience in Ontario demonstrated that waste trading partners will not transition to e-manifests without a regulatory/financial incentive. This was true even though e-manifests deliver cost savings of about \$75/manifest transaction.

As noted in the Section 6.4.2.6, regulations will establish a fee program for manifest processing. The fee for processing a paper manifest will be set higher than the fee for an e-manifest to encourage e-manifest use. The e-manifest transaction processing fee will be shared by waste generators and waste management firms, the major beneficiaries of an e-manifest program. However, hazardous waste e-manifest regulatory fee allocation will reflect the relative e-manifest cost savings of the parties. The waste management firms – the primary financial beneficiary of an e-manifest program – will likely assume the larger portion of the incremental cost of using paper manifests.



Appendix A

United State Environmental Protection Agency

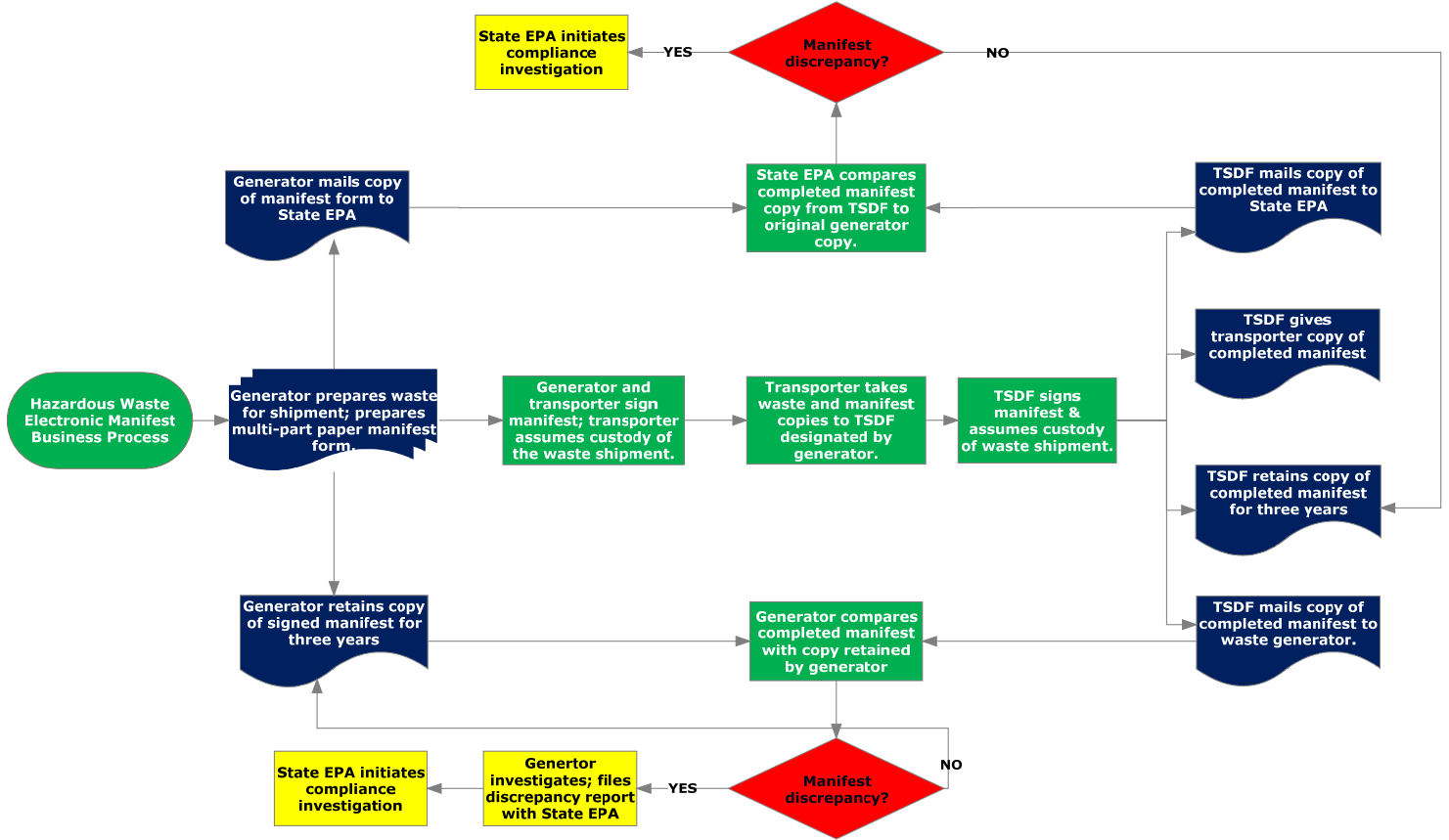
Hazardous Waste Manifest Regulations and Business Processes

Please print or type. (Form designed for use on elite (12-pitch) typewriter.) Form Approved. OMB No. 2050-0039

UNIFORM HAZARDOUS WASTE MANIFEST		1. Generator ID Number	2. Page 1 of	3. Emergency Response Phone	4. Manifest Tracking Number		
5. Generator's Name and Mailing Address		Generator's Site Address (if different than mailing address)					
Generator's Phone:							
6. Transporter 1 Company Name		U.S. EPA ID Number					
7. Transporter 2 Company Name		U.S. EPA ID Number					
8. Designated Facility Name and Site Address		U.S. EPA ID Number					
Facility's Phone:							
GENERATOR	9a. HM	9b. U.S. DOT Description (including Proper Shipping Name, Hazard Class, ID Number, and Packing Group (if any))	10. Containers No. Type		11. Total Quantity	12. Unit WL/VOL	13. Waste Codes
	1.						
	2.						
	3.						
	4.						
14. Special Handling Instructions and Additional Information							
<p>15a. GENERATOR'S/OFFEROR'S CERTIFICATION: I hereby declare that the contents of this consignment are fully and accurately described above by the proper shipping name, and are classified, packaged, marked and labeled/discarded, and are in all respects in proper condition for transport according to applicable international and national governmental regulations. If export shipment and I am the Primary Exporter, I certify that the contents of this consignment conform to the terms of the attached EPA Acknowledgment of Consent.</p> <p>I certify that the waste minimization statement identified in 40 CFR 262.27(a) (if I am a large quantity generator) or (b) (if I am a small quantity generator) is true.</p>							
Generator's/Officer's Printed/Typed Name		Signature		Month		Day	Year
TRANSPORTER	16. International Shipments <input type="checkbox"/> Import to U.S. <input type="checkbox"/> Export from U.S.		Port of entry/exit: _____				
	Transporter signature (for exports only): _____		Date leaving U.S.: _____				
	17. Transporter Acknowledgment of Receipt of Materials		Signature		Month		Day
Transporter 1 Printed/Typed Name		Signature		Month		Day	Year
Transporter 2 Printed/Typed Name		Signature		Month		Day	Year
DESIGNATED FACILITY	18. Discrepancy						
	18a. Discrepancy Indication Space <input type="checkbox"/> Quantity <input type="checkbox"/> Type <input type="checkbox"/> Residue <input type="checkbox"/> Partial Rejection <input type="checkbox"/> Full Rejection						
	18b. Alternate Facility (or Generator)		Manifest Reference Number:		U.S. EPA ID Number		
	Facility's Phone:						
	18c. Signature of Alternate Facility (or Generator)		Signature		Month		Day
19. Hazardous Waste Report Management Method Codes (i.e., codes for hazardous waste treatment, disposal, and recycling systems)							
1.		2.		3.		4.	
20. Designated Facility Owner or Operator: Certification of receipt of hazardous materials covered by the manifest except as noted in Item 18a							
Printed/Typed Name		Signature		Month		Day	Year

EPA Form 8700-22 (Rev. 3-05) Previous editions are obsolete.

DESIGNATED FACILITY TO DESTINATION STATE (IF REQUIRED)



Section 3.2000 Cross Media Environmental Reporting Rule
October 13, 2005

Sec. 3.2000 What are the requirements authorized state, tribe, and local programs' reporting systems must meet?

(a) Authorized programs that receive electronic documents in lieu of paper to satisfy requirements under such programs must:

- (1) Use an acceptable electronic document receiving system as specified under paragraphs (b) and (c) of this section; and
- (2) Require that any electronic document must bear the valid electronic signature of a signatory if that signatory would be required under the authorized program to sign the paper document for which the electronic document substitutes.

(b) An electronic document receiving system that receives electronic documents submitted in lieu of paper documents to satisfy requirements under an authorized program must be able to generate data with respect to any such electronic document, as needed and in a timely manner, including a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that

- (1) The electronic document was not altered without detection during transmission or at any time after receipt;
- (2) Any alterations to the electronic document during transmission or after receipt are fully documented;
- (3) The electronic document was submitted knowingly and not by accident;
- (4) Any individual identified in the electronic document submission as a submitter or signatory had the opportunity to review the copy of record in a human-readable format that clearly and accurately associates all the information provided in the electronic document with descriptions or labeling of the information and had the opportunity to repudiate the electronic document based on this review; and

(5) In the case of an electronic document that must bear electronic signatures of individuals as provided under paragraph (a)(2) of this section, that:

(i) Each electronic signature was a valid electronic signature at the time of signing;

(ii) The electronic document cannot be altered without detection at any time after being signed;

(iii) Each signatory had the opportunity to review in a human-readable format the content of the electronic document that he or she was certifying to, attesting to or agreeing to by signing;

(iv) Each signatory had the opportunity, at the time of signing, to review the content or meaning of the required certification statement, including any applicable provisions that false certification carries criminal penalties;

(v) Each signatory has signed either an electronic signature agreement or a subscriber agreement with respect to the electronic signature device used to create his or her electronic signature on the electronic document;

(vi) The electronic document receiving system has automatically responded to the receipt of the electronic document with an acknowledgment that identifies the electronic document received, including the signatory and the date and time of receipt, and is sent to at least one address that does not share the same access controls as the account used to make the electronic submission; and

(vii) For each electronic signature device used to create an electronic signature on the document, the identity of the individual uniquely entitled to use the device and his or her relation to any entity for which he or she will sign electronic documents has been determined with legal certainty by the issuing state, tribe, or local government. In the case of priority reports identified in the table in Appendix 1 of Part 3, this determination has been made before the electronic document is received, by means of:

(A) Identifiers or attributes that are verified (and that may be re-verified at any time) by attestation of disinterested individuals to be uniquely true of (or attributable to) the individual in whose name the application is submitted, based on information or objects of independent origin, at least one item of which is not subject to change without governmental action or authorization; or

(B) A method of determining identity no less stringent than would be permitted under paragraph (b)(5)(vii)(A) of this section; or

(C) Collection of either a subscriber agreement or a certification from a local registration authority that such an agreement has been received and securely stored.

(c) An authorized program that receives electronic documents in lieu of paper documents must ensure that:

(1) A person is subject to any appropriate civil, criminal penalties or other remedies under state, tribe, or local law for failure to comply with a reporting requirement if the person fails to comply with the applicable provisions for electronic reporting.

(2) Where an electronic document submitted to satisfy a state, tribe, or local reporting requirement bears an electronic signature, the electronic signature legally binds or obligates the signatory, or makes the signatory responsible, to the same extent as the signatory's handwritten signature on a paper document submitted to satisfy the same reporting requirement.

(3) Proof that a particular electronic signature device was used to create an electronic signature that is included in or logically associated with an electronic document submitted to satisfy a state, tribe, or local reporting requirement will suffice to establish that the individual uniquely entitled to use the device at the time of signature did so with the intent to sign the electronic document and give it effect

(4) Nothing in the authorized program limits the use of electronic documents.

<http://www.epa.gov/fedrgstr/EPA-WASTE/2005/March/Day-04/f1966.htm>
Federal Register March 4, 2005

ENVIRONMENTAL PROTECTION AGENCY
40 CFR Parts 260, 261, 262, 263, 264, 265, and 271
[FRL-7867-4]
RIN 2050-AE21

Hazardous Waste Management System; Modification of the Hazardous Waste Manifest System

AGENCY: Environmental Protection Agency.
ACTION: Final rule.

Pages 10792-10794

4. Offerors and the Preparation of Hazardous Waste Shipments and Manifests. The proposed rule would have added a new definition of "preparer" to the definitions in 40 CFR 260.10. While this new definition was proposed in the context of those using an electronic manifest, the purpose of the definition was to extend to the electronic manifest sufficient flexibility to enable the person performing the steps necessary to prepare a waste shipment for transportation to also prepare and sign the electronic manifest on behalf of the generator.

The discussion in the NPRM of the proposed "preparer" definition referred to the instructions for Item 16 of the current manifest paper form as a precedent for this flexibility in the paper context, since the Item 16 instruction allows signatures on the generator certification statement to be made "on behalf of" the generator. Thus, this aspect of the proposed rule raised an issue dealing with the activities of shipment preparers, their authority to initiate and sign the manifest for the generator, and their resulting responsibilities.

Similarly, in the context of TSDFs rejecting waste shipments and preparing manifests to forward rejected waste to alternate facilities (or return the shipment to the generator), the NPRM raised the issue of the responsibility and liability of the rejecting TSDF when it initiates a new manifest and signs the generator's certification statement. For the latter issue, we proposed that the TSDF in such cases was signing the manifest in the capacity of an "offeror" of the shipment, but we asked for comment whether the TSDF forwarding a rejected waste under a new manifest should be viewed instead as signing the manifest as the agent of the generator. Today's final rule affirms that the TSDF rejecting waste and completing a new manifest to track the rejected waste to an alternate facility (or the generator site) signs the manifest in the capacity as offeror of the shipment, and not as an agent of the generator. Nor would the TSDF be functioning as a generator by initiating such a manifest, although the NPRM would have had the facility sign the Generator's Certification statement. The specific issue of TSDFs rejecting wastes and their offeror responsibilities when they complete and sign new manifests is addressed in detail in section IV.B.3. of this preamble. However, because the offeror concept carries broader implications for hazardous waste shipments and waste handlers, and overlaps with the "preparer" concept that we proposed in the May, 2001 NPRM, we are including additional discussion here of the offeror status and how it impacts more generally those who prepare hazardous waste shipments and manifests for transportation.

The term "offeror" refers to a status that is well understood under the Hazardous Materials Regulations (HMRs) of the Department of Transportation (DOT). The HMRs apply to persons who transport hazardous materials in commerce, as well as to persons who offer hazardous materials for transportation. Since hazardous wastes are also hazardous materials within the scope of the HMRs, and since our RCRA statute requires us to regulate hazardous waste transportation-related activities consistent with DOT regulations, the requirements and policies adopted in the HMRs with respect to those who offer hazardous materials for transportation ("offerors") apply to hazardous waste shipments and those who offer hazardous wastes in transportation. DOT consistently has interpreted the "offeror" status as connoting those persons involved with performing certain "pre-transportation" functions that must occur before hazardous materials are transported in commerce. Over the years, DOT has described the pre-transportation functions that may be performed by an "offeror" as including activities such as determining a material's hazard class, selecting a packaging, making and labeling a package, filling a hazardous materials package, preparing a hazardous materials shipping paper (including the hazardous waste manifest), providing emergency response information, and certifying that a hazardous material is in proper condition for transportation in conformance with the HMRs. The latter certification is in fact made when one signs the shipper's certification on a hazardous materials shipping paper, which occurs with respect to the hazardous waste manifest when one signs the Generator's Certification statement. DOT has issued interpretive letters and policy statements respecting offerors and their responsibilities when they perform the types of pre-transportation activities described above. However, these activities and responsibilities were further clarified by DOT when the Department codified these policies in a recent final regulation dealing with the applicability of the HMRs to loading, unloading, and storage. See 68 FR 61906 (October 30, 2003). In this rule, DOT codified a new regulatory definition of "pre-transportation function," and listed the above-described activities and others as examples of these functions that are specified in the HMR and "required to assure the safe transportation of a hazardous material in commerce." See 49 CFR

171.8.

In the preamble discussion of the "pre-transportation functions," DOT explains that a pre-transportation function is performed to prepare a hazardous material and its accompanying shipping documentation for transportation and is required to assure its safe transportation in commerce. 68 FR 61906 at 61909. The rule further explains that it does not matter if the pre-transportation function is performed by the shipper's (generator's) personnel or by the carrier's (transporter's) personnel. The HMR requirements apply to any person who performs or is responsible for performing the pre-transportation functions, and that person must perform the functions in accordance with the HMRs. See 68 FR at 61909-61911. Moreover, as to when compliance or non-compliance must be demonstrated, DOT has stated that it would generally expect an offeror to be able to demonstrate compliance with all applicable pre-transportation requirements at the time the hazardous material is staged for loading and the shipping paper is signed, as this is the offeror's certification that the material has been prepared properly for transportation in accordance with the HMRs. Id. at 61911-61912. At the same time, however, DOT has clarified that "intermediaries" who certify as the offeror assume responsibility only "on behalf of" for all aspects of that shipment about which he knew or should have known."

EPA is today clarifying that the issues concerning the activities of shipment "preparers" and the corresponding issues tied with the authority of a generator or other preparer to complete and sign the Generator's Certification statement on the manifest are governed by the same considerations discussed by DOT with respect to "offerors" and the performance of the pre-transportation functions described in 49 CFR

171.8. Since hazardous waste shipments and waste handlers are subject to the HMRs, and DOT recently has finalized a rulemaking under the HMRs which provides more clarity on these issues, EPA is deferring to these DOT requirements, rather than adopting its own definitions or differing interpretations based on the "on behalf of" language in the manifest instructions or on "preparer" signatures, etc.

Therefore, this final rule resolves the issues pending in this rulemaking relating to preparers signing manifests and TSDFs initiating new rejected waste manifests consistent with the DOT requirements in the HMRs pertaining to offerors and pre-transportation functions. Moreover, we have amended the Generator's Certification statement on the manifest form so that it will be described on the revised form as the Generator's/Offeror's Certification. This change more accurately represents the fact that the person signing the certification statement may in some instances be an offeror involved with the preparation of the waste shipment (or of the manifest) for transportation, rather than the waste generator.

While the proposed rule discussed the offeror status while dealing with the issue of TSDFs rejecting and re-shipping wastes, we wish to emphasize that the offeror concept is broad enough to cover many waste shipment scenarios. Indeed, the offeror status and signature would be encountered most commonly in connection with the waste pick-up and transportation arrangements made between generators and waste transporters when the transporters service the generators' sites. Since the transporter's personnel frequently will aid generators in preparing their waste shipments for transportation (e.g., selecting packages, labeling containers, filling and closing containers, selecting and affixing placards, completing the manifest or reviewing it for compliance with the HMRs and RCRA), the transporter performing such pre-transportation functions may be an offeror with respect to the shipment. While a generator may certainly sign the generator certification statement in its capacity as the generator, today's rule is intended to clarify that another person, such as a transporter making a waste pick-up and helping with the pre-transportation functions, may sign the certification statement on the manifest in their capacity as an offeror. This person may sign as an offeror if they have performed pre-transportation functions, and can certify that the shipment has been properly described, classified, packed, marked, and labeled, and is in all respects in proper condition for transportation under the applicable international or national regulations. The person preparing the shipment and making the certification is responsible for the proper discharge of the offeror functions they perform and the truth of the certification statement. The offeror is liable in its independent offeror capacity for discharging their offeror responsibilities, regardless of whether or not they may also be viewed as performing these activities "on behalf of" or the agent of the generator, as the generator's independent service contractor, or pursuant to a course of dealing with the generator.

Because we believe that the "offeror" approach and the new regulatory requirements in the HMRs concerning pre-transportation functions deal effectively with the issues we raised in the NPRM with respect to shipment preparers and manifest signatures, we are not finalizing the definition of "preparer" we proposed for inclusion in Sec. 260.10. Nor are we expanding or otherwise modifying the meaning of the language in the Item 16 manifest form instruction enabling one to include the words "on behalf of" in connection with a signature, although it will now apply both to generator and offeror signatures. A preparer who assists with pre-transportation functions under the HMRs, and who can certify to the "shipper's certification" statements in the Generator's/Offeror's Certification, may sign this certification and initiate the manifest as an offeror. The "on behalf of" language is retained in the instruction to the signature item in order to effectuate the limited purpose for which this language was added in

1986, that is, to connote that generator (and now offeror) organizations typically act through their employees or agents, and that the employee/agent signatures bind the organizations they represent.

The term "offeror" thus connotes a status in hazardous materials management distinct from that of a shipper or generator. The offeror's responsibilities are limited to the proper discharge of the pre-transportation functions they perform or certify to being properly performed. While it is true that a generator may often elect to perform the pre-transportation functions, these represent only a subset of the full generator responsibilities set out in 40 CFR part 262. Likewise, when an entity other than a generator (e.g., transporter or TSDF) performs pre-transportation functions as an offeror, it does not thereby assume full generator responsibilities. Rather, it assumes only the more limited responsibilities (for the pre-transportation functions) and the distinct liability that attaches to the offeror status. Therefore, a TSDF that only is offering hazardous waste in transportation after rejecting and staging the waste temporarily at its facility would be subject to the offeror responsibilities for the new movement of the waste, but it would not be subject to the full range of generator requirements. This issue is explained further in section IV.B.3. of this preamble.

<http://www.epa.gov/fedrgstr/EPA-WASTE/2008/February/Day-26/f3615.htm>

Federal Register
ENVIRONMENTAL PROTECTION AGENCY
40 CFR Parts 260, 261, 262, 263, 264, 265, and 271
[EPA-HQ-RCRA-2001-0032; FRL-8534-1]
RIN 2050-AG20

Hazardous Waste Management System; Modification of the Hazardous Waste Manifest System

AGENCY: Environmental Protection Agency (EPA).
ACTION: Notice of data availability and request for comment.
February 26, 2008

EPA agrees with waste management industry and state government commenters' concern that it would not be efficient to have an electronic manifest system collecting data only from electronic manifests, while another paper-based system addresses the data only from paper manifests. Therefore, we believe that the system being designed should be a unified system for processing and distributing data from all manifests, including data from paper manifests. We considered several options aimed at simplifying the process for collecting paper forms and at ensuring that the data collected from both electronic manifests and paper forms could be efficiently processed so that a comprehensive set of manifest data would be available to users and regulators. We have identified a preferred approach that we believe provides the most efficient solution to the dual paper/electronic systems problem.

Under our preferred approach, the final destination facility (i.e., designated final TSDF), for each hazardous waste shipment involving a paper manifest, would be required to submit the top copy (i.e., Page 1 of the 6-page set) of the paper manifest form to the e-Manifest system operator within 30 days of receipt of the waste shipment. While the e-Manifest system is not yet designed, we envision that the designated facility could mail a copy to the e-Manifest system operator or could transmit an image file to the EPA system so that the e-Manifest system operator could key in the data from the paper copies or image files to the data system. Alternatively, the designated facility could submit both the image file and a file presenting the manifest data to the system in image file and data file formats acceptable to the e-Manifest system operator and supported by the Central Data Exchange (CDX). For paper copies mailed to the system by designated facilities, the e-Manifest system operator would create or obtain an image file of each such manifest, and store it on the system for retrieval by state or federal regulators. The e-Manifest system operator also would key in, electronically scan using an optical character recognition (OCR) device, or otherwise transfer the federal- and state-regulated waste data from these paper copies to the e-Manifest system. By having all manifest data in electronic form, EPA could extract any data regarding RCRA hazardous wastes for inclusion in its data systems, while the states could pull off data from the system concerning both federally regulated RCRA and state-regulated wastes for processing in the states' own tracking systems.

We envision that designated facilities would be required to pay a fee to the system operator for processing the data from these final copies of the paper forms, and the fee would presumably vary with the type of submission (mailed copy, image file, or image plus data file), as these submission types would likely present a different level of effort insofar as the processing steps required to enter the form data into the system. It is likely that the fee paid by the designated facility would be passed on to the generator (i.e., the designated facility's customer). We estimate that the paperwork burden cost to TSDFs for submitting a copy of the final manifest could be \$1.95 per paper manifest, for an incremental (i.e., over current baseline) annual cost to TSDFs of between \$1.6 million and \$6.5 million per year. In addition, we estimate the possible fee that EPA's e-Manifest system operator (or other EPA-designated e-Manifest affiliate) might charge TSDFs for receiving paper manifests and for transferring (i.e., imaging and keypunching) paper manifest data to the e-Manifest system, could be between \$0.25 to \$0.75 per paper manifest, for an incremental (i.e., over current baseline) annual cost to TSDFs of between \$0.2 million and

\$2.9 million. On a combined basis, we estimate these two components of paper manifest processing incremental costs to TSDFs could total between \$1.8 million and \$9.4 million annually, representing an average incremental cost to TSDFs of \$2.20 to \$2.70 per paper manifest. We invite public comment on our approach and the cost estimates.

We believe such an approach simplifies manifest copy submissions for the regulated TSDFs, who in the future would only need to provide designated facility copies to one location--the national centralized e-Manifest system--rather than supply copies to the numerous state agencies that now collect a copy of the final manifest. Further, it focuses the federal collection effort on a copy of the final paper manifest forms from the designated facilities, which provide the best accounting of the quantities and types of hazardous wastes that were actually received for management. We believe that providing a means to collect a complete set of hazardous waste receipts data from RCRA TSDFs (the merged set of paper and electronic manifest data), also may in the future provide EPA with the means to replace biennial reporting by TSDFs of waste receipts data with a much simpler approach that relies upon the designated facility data reported to the e-Manifest system.

We also believe that there are a number of benefits of this approach to state programs. As states are connected to the e-Manifest system through EPA's National Environmental Information Exchange Network, they would be able to pull off the image files and the data keyed from paper manifests from this central processing service, just as they would be able to obtain the data and presentations of electronic manifests from the eXtensible Markup Language (XML) schemas and stylesheets transmitted on the e-Manifest system. This national data system also presents a much more efficient approach that can eliminate the need for discrete state systems designed to capture manifest data.

In addition, as the e-Manifest system operator would be able to assess appropriate fees for the paper processing and data entry activities necessary to process the data from paper forms and enter them into the e-Manifest system, the actual costs of providing these services would be recovered by the system operator from the designated facility. Since we expect that electronic manifests will be much more efficient to process than paper forms, the differential fees that are established for paper and electronic manifest processing likely would operate as an additional incentive for the transition to electronic manifests.

While we intend to clarify in the final rule that the use of the electronic manifest format would be optional for members of the regulated community, our preferred approach to collect a copy of the final paper manifest forms from designated facilities and to process the data from these paper forms centrally means that these designated facilities will be required to interact with the e-Manifest system (i.e., submitting data either electronically or by mail and paying established fees). Thus, this NODA confirms our intention to have a single national hazardous waste database.

Facilities that elect to use the electronic manifest format would submit their manifest information electronically as a natural consequence of participating in the e-Manifest system. The e-Manifest system would be designed for the purpose of distributing electronic manifest data among the users and regulatory agencies, while the electronic manifest information is being obtained, processed, and transmitted electronically via the e-Manifest system. On the other hand, those facilities and hazardous waste handlers that choose to use the paper manifest forms or are presented with paper forms rather than electronic manifest formats, would need to process the paper manifest forms physically in the conventional manner that has been the norm since the uniform hazardous waste manifest form was introduced in 1984. However, in place of sending a copy of the final manifest directly to the destination state, the final rule would require the designated facility to send Copy 1 of the paper manifest form to EPA's e-Manifest system operator. Thus, the designated facilities would be required to submit a copy of the final manifest to the e-Manifest system, either in the supported electronic format or as a paper copy, and pay a fee for this service. In other words, the use of the electronic manifest format would be voluntary under the final rule, although the submission of either a completed paper or electronic manifest to the EPA system operator and payment of an associated fee in every case would be required of designated facilities. Once this requirement is effective, and all copies of the final manifest (electronic or paper) from designated facilities are being submitted directly to EPA's e-Manifest system operator, the states would be able to obtain their copies of the final manifest and data from the e-Manifest system through their computer systems on the National Environmental Information Exchange Network. It is EPA's intent that the submission of the final paper manifest copy to the e-Manifest system would replace the requirement to supply paper manifests directly to the states. Since the states would have nodes in place on the Exchange Network for receiving manifest copies from the system, it would no longer be necessary for the states to require the direct submission of paper copies to the states. Thus, the paper copy submission requirement could replace the requirement for facilities to submit copies of the final manifest to the states. Note that the facilities that receive paper manifests will still need to retain a paper manifest copy among their own facility records for the 3-year record retention period in accordance with current requirements. We request comment on our recommendation to collect a copy of the final electronic and paper manifest forms from designated facilities and to process the data from these forms centrally.

JUN 26 2008



**Transportation
Security
Administration**

Dear Highway and Motor Carrier Stakeholders:

The Transportation Security Administration (TSA) is providing security action items for the highway transportation of specific hazardous material substances as listed in appendices A and B of this document. Adoption of these measures is voluntary.

Movement of certain quantities of Tier 1 Highway Security-Sensitive Materials (HSSM) or Tier 2 HSSM by highway motor vehicle warrants special consideration and attention. These materials have the potential to cause significant fatalities and injuries or significant economic damage when released or detonated during a transportation security incident. The voluntary security practices contained in Appendix A have been developed by the TSA Office of Transportation Sector Network Management, Highway and Motor Carrier Division, in conjunction with stakeholders including representatives of the chemical manufacturing industry, chemical carriers and transportation industry, as well as appropriate Federal agencies. Appendix B provides a listing of Tier 1 and Tier 2 HSSM. TSA remains solely responsible for the contents of these documents. The list of substances in Appendix B is not intended to meet the requirement for the development of Security-Sensitive Materials under the *Implementing Recommendations of the 9/11 Commission Act of 2007*.

The efficient operation of our critical interstate and intrastate highway system requires a uniform nationwide approach to highway motor carrier security. In addition to collaboration with the chemical manufacturing industry and chemical carriers, TSA also gathered security information during its Corporate Security Review, which, among other areas, identified common security practices within the hazardous material motor carrier industry. These security action items have been developed by TSA in consultation with the Pipeline and Hazardous Material Safety Administration (PHMSA) and the Federal Motor Carrier Safety Administration (FMCSA), and build upon existing PHMSA and FMCSA hazardous materials regulations. In particular the PHMSA regulations in title 49, Code of Federal Regulations, sections 172.704 and 172.800 require each transporter of hazardous materials to develop and implement security plans and to train appropriate employees in security measures. TSA is providing these voluntary security practices as measures that should be considered for implementation by motor carriers transporting Tier 1 HSSM and Tier 2 HSSM. If the motor carrier adopts these security practices, TSA recommends that the practices be included in security plans when they are developed, implemented, and revised. The security practices are voluntary to allow highway motor carriers to adopt measures best suited to their particular circumstances provided the measures are consistent with existing regulations, laws, or directives.

The security action items have been divided into four categories 1) general security; 2) personnel security; 3) unauthorized access; and 4) en route security. General security measures pertain to security threat assessments, security planning, protecting critical information, and awareness of industry security practices. Personnel security and unauthorized access refer to practices affecting the security of the motor carrier's employees, contracted employees, and its property. En route security refers to the actual movement and handling of motor vehicles containing HSSM.

TSA recognizes that no one solution fits all motor carriers and circumstances. These security action items allow for flexibility in implementation based upon the assessed vulnerability of a particular process or operation. Where appropriate, implementation of these action items to their fullest extent practicable should be the goal of the affected owner and operator.

TSA plans to monitor the use and effectiveness of these security action items and to revise them as circumstances warrant. TSA encourages members of the affected industry and Federal agencies to provide feedback to TSA Highway and Motor Carrier Division. Questions and comments may be provided at highwaysecurity@dhs.gov

Questions may be directed to Mr. William Arrington, General Manager, Highway and Motor Carrier Division, Transportation Security Administration, TSA-28, 601 South 12th Street, Arlington, VA 22202.

Sincerely yours,



John P. Sammon
Assistant Administrator
Transportation Sector Network Management

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) Transported by Motor Carrier

Attachment 1 to Appendix A - TSA Highway and Motor Carrier Division Guidance for Background Checks for Motor Vehicle Hazmat Employees other than Motor Vehicle Drivers

Appendix B – List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM) with Corresponding Security Action Items

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.

Attachment 1 to Appendix A
Security Action Items
Guidance for Background Checks for
Motor Vehicle Hazmat Employees other than Motor Vehicle Drivers

The Transportation Security Administration is concerned about the risk posed by the transportation by motor carrier over the nation's highways of Tier 1 Highway Security-Sensitive Materials (Tier 1) and Tier 2 Highway Security-Sensitive Materials (Tier 2) as defined in this guidance. While individuals with a commercial driver's license with a hazardous materials endorsement are the subject of mandatory background checks, other employees involved in the transportation of certain hazardous materials by motor vehicle are not subject to background checks. This document provides guidance on voluntarily conducting background checks for motor vehicle hazmat employees other than motor vehicle drivers holding a valid commercial driver's license with a hazardous materials endorsement. This guidance is not intended to supersede or conflict with Federal or State.

Criminal History Checks

Many highway transportation sector hazmat employers may use criminal background checks to assess the suitability of their employees for positions. To the extent that a highway transportation sector hazmat employer chooses to do so for employees with unmonitored access to company-designated critical infrastructure, they should consider using the federally established list (attached) of disqualifying crimes applicable to hazmat drivers and transportation workers at ports (see 49 CFR 1572.103).¹

Verification of Social Security Number

In addition, the highway transportation sector hazmat employer should consider using the Social Security Number Verification System (SSNVS) that the Social Security Administration (SSA) makes available to all employers. Employers can verify that current employee names and social security numbers match the SSA's records. This reduces the likelihood that an individual who has adopted a false identity.

Verification of Immigration Status

The highway transportation sector hazmat employer should also consider using the Systematic Alien Verification for Entitlements (SAVE) database to determine a non-citizen's immigration status. SAVE is an intergovernmental information-sharing service for agencies and employers to use to ensure that an applicant has lawful presence in the United States. SAVE is nationally accessible and contains selected immigration status information on approximately 50 million individual non-citizens.²

¹ See 72 FR 3492 (January 25, 2007), as corrected by 72 FR 5632 (February 7, 2007)

² For information on accessing SAVE, contact: Director, SAVE Program, USCIS SAVE Program, Douglas Development Building, 2nd Floor, 20 Massachusetts Ave., NW, Washington, DC 20529.

**Attachment 1 to Appendix A
Security Action Items
Guidance for Background Checks for
Motor Vehicle Hazmat Employees other than Motor Vehicle Drivers**

Redress Procedures

A highway transportation sector hazmat employer should consider establishing an internal redress process for adversely affected applicants and personnel, including an appeal and waiver process similar to the system established for holders of a commercial drivers license and transportation workers at ports (see 49 CFR Part 1515).

An appeal process could be designed to provide an applicant or personnel with the opportunity to show that he or she does not have a disqualifying conviction by correcting outdated underlying court records or proving mistaken identity.

A waiver process could be designed to provide an applicant or personnel with the opportunity to be hired or continue employment by demonstrating rehabilitation or facts surrounding a conviction that mitigate security concerns. The highway transportation sector hazmat employer should consider permitting an applicant or personnel to submit information pertaining to any of the following:

1. Circumstances of the disqualifying offense;
2. Restitution made;
3. Letters of reference from clergy, employers, probation/parole officers; and
4. Other factors the individual believes bear on his or her good character.

The highway transportation sector hazmat employer may elect to incorporate the redress process into the disciplinary procedures already in use as part of its management or labor relations procedures.

Document: S:\TSASharedFolders\TSNM\HighWay\Programs\HAZSUBS & Chemicals\HSHM_SSHM_SAI\Final_Hazmat_SAI_Documents_3-25-08\TSA-080429-001_D1 Appendix A-1_HSSM_SAI_#6_rev4_final_04-29-08.doc

Attachment 1 to Appendix A
Security Action Items
Guidance for Background Checks for
Motor Vehicle Hazmat Employees other than Motor Vehicle Drivers

49 CFR Part 1572 Subpart B – Standards, Appeals, and Waivers for Security Threat Assessments (Source: 72 FR 3492, Jan. 25, 2007; 72 FR 5633, Feb. 7, 2007)

Sec. 1572.103 Disqualifying Criminal Offenses.

(a) *Permanent disqualifying criminal offenses.* An applicant has a permanent disqualifying offense if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following felonies:

- (1) Espionage or conspiracy to commit espionage.
- (2) Sedition, or conspiracy to commit sedition.
- (3) Treason, or conspiracy to commit treason.
- (4) A federal crime of terrorism as defined in 18 U.S.C. 2332b(g), or comparable State law, or conspiracy to commit such crime.
- (5) A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101. The term “economic disruption” does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employer-employee dispute.
- (6) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a State law that is comparable.
- (7) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).
- (8) Murder.
- (9) Making any threat, or maliciously conveying false information knowing the same to be false, concerning the deliverance, placement, or detonation of an explosive or other lethal device in or against a place of public use, a state or government facility, a public transportation system, or an infrastructure facility.
- (10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq, or a comparable State law that is comparable, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the crimes listed in paragraph (a) of this section.
- (11) Attempt to commit the crimes in paragraphs (a)(1) through (a)(4).
- (12) Conspiracy or attempt to commit the crimes in paragraphs (a)(5) through (a)(10).

(b) *Interim disqualifying criminal offenses.* (1) The felonies listed in paragraphs (b)(2) of this section are disqualifying, if either:

- (i) the applicant was convicted, or found not guilty by reason of insanity, of the crime in a civilian or military jurisdiction, within seven years of the date of the application; or
- (ii) the applicant was incarcerated for that crime and released from incarceration within five years of the date of the TWIC application.

(2) The interim disqualifying felonies are:

Attachment 1 to Appendix A
Security Action Items
Guidance for Background Checks for
Motor Vehicle Hazmat Employees other than Motor Vehicle Drivers

- (i) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.
 - (ii) Extortion.
 - (iii) Dishonesty, fraud, or misrepresentation, including identity fraud and money laundering where the money laundering is related to a crime described in paragraphs (a) or (b) of this section. Welfare fraud and passing bad checks do not constitute dishonesty, fraud, or misrepresentation for purposes of this paragraph.
 - (iv) Bribery.
 - (v) Smuggling.
 - (vi) Immigration violations.
 - (vii) Distribution of, possession with intent to distribute, or importation of a controlled substance.
 - (viii) Arson.
 - (ix) Kidnapping or hostage taking.
 - (x) Rape or aggravated sexual abuse.
 - (xi) Assault with intent to kill.
 - (xii) Robbery.
 - (xiii) Fraudulent entry into a seaport as described in 18 U.S.C. 1036, or a comparable State law.
 - (xiv) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq., or a comparable State law, other than the violations listed in paragraph (a)(10) of this section.
 - (xv) Conspiracy or attempt to commit the crimes in this paragraph (b).
- (c) *Under want, warrant, or indictment.* An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in this section, is disqualified until the want or warrant is released or the indictment is dismissed.
- (d) *Determination of arrest status.* (1) When a fingerprint-based check discloses an arrest for a disqualifying crime listed in this section without indicating a disposition, TSA will so notify the applicant and provide instructions on how the applicant must clear the disposition, in accordance with paragraph (d)(2) of this section.
- (2) The applicant must provide TSA with written proof that the arrest did not result in conviction for the disqualifying criminal offense, within 60 days after the service date of the notification in paragraph (d)(1) of this section. If TSA does not receive proof in that time, TSA will notify the applicant that he or she is disqualified. In the case of an HME, TSA will notify the State that the applicant is disqualified, and in the case of a mariner applying for TWIC, TSA will notify the Coast Guard that the applicant is disqualified.

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Division 1.1 Explosives	Any quantity	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Division 1.2 Explosives	Any quantity	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Division 1.3 Explosives	Any quantity	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
Division 1.4 Explosives	Not subject other than Division 1.4 Explosives specified by UN number below.																									
Division 1.4B Explosives	Any quantity of the following explosives : UN No. 0361, 0365, 0255, 0267		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 1.4S Explosives	Any quantity of the following explosives: UN No. 0500, 0366, 0456, 0455, 0441		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 1.4D Explosives	Any quantity of the following explosives: UN No. 0289, 0104, 0237, 0440		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 1.5 Explosives	Any quantity		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Division 1.6 Explosives	Not Subject																									
Division 2.1 Flammable Gases (for def, see 49 CFR 173.115 and 173.116)	Single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X							
Division 2.2 Non- Flammable Gases	Not subject other than Division 2.2 substances specified below																									
Division 2.2 Non- Flammable Gas (also meeting the definition of a material poisonous by inhalation ¹)	Anhydrous ammonia (UN 1005) in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs) ⁱⁱ	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Division 2.2 Non-Flammable Gas (with a subsidiary hazard of Oxidizer (Division 5.1)) ⁱⁱⁱ	Substances with subsidiary hazard of Oxidizer (Division 5.1) in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 2.3 Toxic (Poison) Gas	Hazard zone A & B ≥ 5 lbs. in a single package.	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Division 2.3 Toxic (Poison) Gas	Hazard zone C & D in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs).	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Class 3 Flammable Liquids	PG I and II in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Class 3 Flammable Liquids	Any quantity desensitized explosives		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation ^{iv})	PG I in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Division 4.1 Flammable Solids (Desensitized Explosives)	Limited to any quantity of desensitized explosives in Division 4.1 including those categorized as Packing Group I and the following Packing Group II materials: UN2555, UN2556, UN2557, UN2907, UN3319, and UN3349. ^v		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 4.2 Spontaneously Combustible Material	Packing groups I and II only in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 4.3 Dangerous When Wet Material	Any quantity		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Division 5.1 Oxidizer	Packing groups I & II in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 5.2 Organic Peroxide	Limited to any quantity of Type B organic peroxide (for def of types, see 49 CFR 173.128), liquid or solid, temperature controlled.		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 6.1 Poisonous Materials	Packing groups I, II and III in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation ^{vi})	Hazard zone A & B ≥ 5 lbs. in a single package	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM	General Security				Personnel Security			Un- Author Access		En-Route Security														
			Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
		1	2																							
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation ^{vii})	Hazard zone C & D in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs).	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Division 6.2 Infectious substances	Select Agents – (As listed by Centers for Disease Control in 43 CFR 73.3)		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X								
Class 7 Radioactive Materials, (10 CFR part 110, Appendix P, Category 1 materials)	International Atomic Energy Agency (IAEA) Code of Conduct Category 1 and 2 materials including Highway Route Controlled quantities as defined in 49 CFR 173.403 or known as radionuclides in forms listed as RAM-QC by the Nuclear Regulatory Commission.	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Class 8 Corrosive Materials	Packing group I in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X								

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM		General Security				Personnel Security			Un- Author Access		En-Route Security													
		Tier		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		1	2																							
Class 8 Corrosive Materials (also meeting the definition of a materials poisonous by inhalation ^{viii})	Packing group I and II in single bulk packaging ≥ 3000 L (792 gal) or 3000 kg (6614 lbs.)	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Class 9	Not Subject																									
Class ORM-D	Not Subject																									
Other Materials	Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules 1, 2, or 3. ^{ix}	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

List of Security Action Items

General Security:

- 1) Security Assessment and Security Plan Requirements.
- 2) Awareness of Industry Security Practices.
- 3) Inventory Control Process.
- 4) Business and Security Critical Information

Personnel Security:

- 5) Possession of a Valid Commercial Drivers License – Hazardous Materials Endorsement.

- 6) Background Checks for Highway Transportation Sector Hazmat Employees other than Motor Vehicle Drivers with a Valid CDL with HME.
- 7) Security Awareness Training for Hazmat Employees.

Unauthorized Access:

- 8) Access Control System for Drivers.
- 9) Access Control System for Facilities Incidental to Transport.

**Appendix B –
List of Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) and
Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)
with Corresponding Security Action Items**

The list of Highway Security Sensitive Materials (HSSM) was prepared by the TSA Transportation Sector Network Management Office

DOT Hazard Class (see 49 CFR 171.8 for definitions of these hazard classes)	Threshold Quantity (unless otherwise noted see 49 CFR 171.8 for definitions)	HS SM	General Security				Personnel Security			Un- Author Access	En-Route Security														
			Tier	1	2	3	4	5	6		7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
		1	2																						

En-Route Security:

- 10) Establish Communications Plan.
- 11) Establish Appropriate Vehicle Security Program.
- 12) Establish Appropriate Cargo Security Program.
- 13) Implement a Seal/Lock Control Program.
- 14) High Alert Level Protocols.
- 15) Establish Security Inspection Policy and Procedures.
- 16) Establish Reporting Policy and Procedures.
- 17) Shipment Pre-Planning, Advance Notice of Arrival, and Receipt of Confirmation Procedures.
- 18) Preplanning Routes.
- 19) Security for Trips Exceeding Driver Hours of Service.
- 20) Dedicated Truck.
- 21) Tractor Activation Capability.
- 22) Panic Button Capability.
- 23) Tractor and Trailer Tracking Systems

^{viii} See 49 CFR 171.8 for the definition of materials poisonous by inhalation

^{ix} Chemicals listed under this designation as Chemicals Weapons Convention are expected to be captured under the previously listed DOT Hazard Classes. They are listed in this Appendix as Other Materials for completeness and are not intended to indicate a new hazard class.

Cross Reference for Security Action Items

Current SAI	Original SAI	Current SAI	Original SAI
1	25	12	8, 12,
2	23	13	9
3	24	14	17, 18
4	26	15	19
5	1	16	20
6	2	17	10
7	3	18	14
8	4	19	15
9	5	20	22
10	6	21 and 22	13
11	7, 8, 11, 12	23	16

ⁱ See 49 CFR 171.8 for the definition of materials poisonous by inhalation

ⁱⁱ TSA recognizes the provisions for agricultural operations contained in 49 CFR 173.5

ⁱⁱⁱ See 49 CFR 171.8 for the definition of subsidiary hazard

^{iv} See 49 CFR 171.8 for the definition of materials poisonous by inhalation

^v For a listing of desensitized explosives see the United Nations Recommendations on the Transport of Dangerous Goods, Volume I, 14th revised edition, paragraph 2.4.2.4.1, definitions

^{vi} See 49 CFR 171.8 for the definition of materials poisonous by inhalation

^{vii} See 49 CFR 171.8 for the definition of materials poisonous by inhalation

Appendix C

High Level Plan for Implementing H.R. 1 (Transportation Sector Network Management; Highway Motor Carrier Programs Office; U.S. Transportation Security Administration)

This paper describes a high level plan for implementing H.R. 1 requirements to establish a HAZMAT Truck Security program.

A. Background

In keeping with the Transportation Security Administration's mission to protect the nation's transportation systems, the United States' Congress has charged the TSA to *develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides: (a) frequent or continuous communications, (b) vehicle position location and tracking capabilities, and (c) a feature that allows a driver of such vehicles to broadcast an emergency distress signal.*

To meet the agency mission, TSA started the HAZMAT Truck Security Pilot project in 2005. Seven tracking vendors and twelve HAZMAT carriers participated in the pilot project. The pilot project will conclude in early 2008.

B. Program Platform

The results of the pilot project have demonstrated a platform for the development of a program satisfying the H.R. 1 requirements:

- **Frequent or continuous communications** – TSA has developed a set of tested protocols that are capable of interfacing with (a) existing truck tracking systems, (b) state/local law enforcement agencies and first responders and (c) with federal intelligence and emergency management centers.
- **Vehicle position location and tracking capabilities** – TSA has implemented a tested and functioning truck tracking center that allows TSA to “continually” monitor truck locations and track load types in all of the continental United States.
- **A feature that allows a driver of such vehicles to broadcast an emergency distress signal** – TSA has developed a concept of operations that has gone through considerable testing and being vetted by government and industry volunteers. This concept of operations facilitates effective responses to drivers' emergency distress signals.

The pilot project has shown that the transition from pilot to program is feasible. It has demonstrated a prototype for a centralized truck tracking center. The truck tracking center was used to coordinate incident response with appropriate first responders and a government intelligence operations center. The truck tracking center system collected data in real-time from carrier-operated systems utilized in the field. Upon receiving an alert notification or upon detection of an abnormal condition, truck tracking center dispatchers helped manage the process of notifying stakeholders and coordinating responses to transportation security incidents.



C. Program Approach

TSA will develop a rollout plan to expand and enhance the following two key areas:

1. System Implementation

Based on the findings of the pilot project, the program will:

- Further develop its standards-based communications interface to adapt to evolving technical and functional requirements.
- Fully develop and implement a scalable truck tracking center to function as a central operations control area to (i) collect data from motor carriers, (ii) monitor events and coordinate a response, and (iii) facilitate communications to support a coordinated response.
- Further refine the systems and algorithms that provide the foundation of truck tracking center system's risk-based approach to transportation event management.

2. Carrier Recruitment

The success of the HAZMAT Truck Security Program will depend on the voluntary involvement and participation of HAZMAT motor carriers and tracking technology vendors. In the program, TSA will actively reach out to industry carriers through individual contacts, conferences, meetings, and associations to promote volunteer participations for the program. In addition, TSA will seek out input from industry to make sure the approach is reasonable and compatible with existing business practices.

D. Next Steps

Through the pilot project, TSA has demonstrated both the feasibility and acceptability of the piloted truck tracking program. During demonstrations to industry representatives, TSA received positive feedback regarding the pilot project. TSA will continue to incorporate industry inputs, further develop the system, and expand carrier participation to establish a program meeting the requirements in H.R. 1 Section 1554.



**Transportation Sector Network Management
Highway & Motor Carrier Programs Office**

Appendix D

FMCSA Functional Specifications for Untethered Trailer Tracking Systems ¹

4.2.1.1 Near real-time trailer identification

Trailer identification is established via position reports sent from the UTT system terminal on the trailer. The UTT system terminal monitors the Global Positioning System (GPS) for its location, checks other on-board sensors, and sends this information over the air (OTA). The information presented to the user includes the trailer identification number (ID) and trailer type, as well as the user Standard Carrier Alpha Code (SCAC). The user can view the host software to find the latest trailer location and status on a map. Trailer locations are displayed relative to predefined landmarks or street or highway intersections. The trailer status refers primarily to three key pieces of information: whether the trailer has cargo or is empty, whether the door is open or closed, and whether the trailer is connected or disconnected to a tractor. If the latest scheduled report is not sufficiently current, the user can request an update from the UTT system terminal. The request will be answered immediately if the terminal is awake. Otherwise, the request will be queued until the next scheduled wake-up time.

- The UTT system allows a user to request and obtain the current trailer status information from the terminal, which includes at minimum the trailer position, cargo status, door status, and status of any other sensors, if installed.
- The UTT terminal shall wake up to listen for status requests at user-configurable intervals, which will include at minimum: never; once per 30 minutes; and once per 1, 2, 6, 8, and 12 hours.
- The UTT terminal shall default to wake up and listen for requests for status once per 6 hours.

4.2.1.2 Time of trailer connection and disconnection

The time of trailer connection and disconnection refers to the time that a trailer is physically connected or disconnected from a tractor. For example, a trailer is typically disconnected from the tractor when the tractor-trailer arrives at a destination where the trailer may be unloaded while the tractor departs to pick up and move another trailer.

- The UTT system shall detect and record time of trailer connections and disconnections.
- The connection and disconnection times recorded by the UTT system shall be accurate within 15 minutes of the actual connection and disconnection times.
- The UTT system connection and disconnection events shall be sent immediately upon validation by default.

4.2.1.3 Trailer location and mapping

Trailer positions are established via GPS or other locating technology. The UTT system terminal is configurable to wake up to check for positions at user-defined intervals. Once the position has been established, the coordinates are reported to the user visually at the carrier site through a map interface. Although latitude and longitude are provided, the user would normally see the trailer's position on a map with reference to highways, streets, intersections, or user-defined landmarks.

- UTT system position reporting intervals shall be user-configurable OTA.
- UTT system position reporting intervals shall be configurable at a minimum to: never; 15 minutes; 1, 6, 8, 12, 24 hours; and then once per day until the 30th day. (Reporting intervals that are more frequent than 15 minutes may be utilized in certain instances, such as trying to locate a stolen trailer.)
- UTT system position reporting intervals of less than 60 minutes shall be configurable by the system administrators only, unless system administrators have given a user the capability to change the position reporting interval to less than 60 minutes. (The purpose of this requirement is to prevent excessive messaging and battery drain, especially for users who may not clearly understand the constraints of the system.)
- The UTT system shall provide a daily interval for position reports by default.

¹ These functional specifications were published in the FMCSA report, Untethered Trailer Tracking and Control System Operational Requirements Document; August 2005. <http://www.fmcsa.dot.gov/facts-research/research-technology/report/untethered/untethered-trailer-tracking.pdf>

- The UTT system shall provide the configurable capability to suppress scheduled position reports when power is detected on Pin 7 of the SAE J560 connector. (The SAE J560 is the standard connector used to connect the electrical system of a trailer to a tractor, and power on Pin 7 may indicate that a tractor is attached to the trailer. If there is a mobile communications system on a tractor tethered to a trailer, position reports may be more cost effectively sent from the tractor system versus the UTT system. When the tractor mobile communications system is non-operational or more frequent trailer positioning updates are required, the UTT system can be effectively utilized to provide this information.)
- The UTT system shall support a mapping module including street-level maps for the United States, Canada, and Mexico.
- The UTT system shall provide visibility to active geo-fences, cargo event locations, door event locations, connection and disconnection locations, and historical positions on maps. (For the UTT system tested in the pilot test, geo-fences will be visible on maps as polygons or circles overlaid on the map, and geo-fence violations will be visible as icons appearing in a line item for a trailer.)
- The UTT system shall allow users to view one or more selected trailers with proximity from pre-defined landmarks on a map display. (For the UTT system tested in the pilot test, there is no maximum limit to the number of trailers that may be displayed on maps, although in an area densely populated with trailers, viewing can be difficult. A pop-up list of 'hidden' trailers provides visibility to the trailers that may be overlapped on the display.)
- The UTT system shall provide the ability for users to view the position history of a trailer on a map display for a user selected period of time or a default setting to the prior week.
- The UTT system software shall support the creation, modification, and deletion of custom landmarks by authorized users.
- The UTT system software shall support the display of trailer positions with proximity to the nearest custom landmark, if configured as such under user's preferences. This allows the user to display all position reports in terms of the trailer's proximity to a landmark.
- The UTT system software shall support the query for trailers near a specified landmark within a specified distance, which allows the user to query for any trailer within a certain distance from a landmark.

4.2.1.4 Geo-fencing

A geo-fence is an electronic boundary that a user can create to monitor trailer location and movement. Geo-fences may be created, viewed, and edited visually on an interactive map. For example, a user could locate a trailer on a map and draw a geo-fence around the trailer position by clicking and dragging a mouse. The geo-fence may be assigned to a trailer or to groups of trailers. Once the geo-fence is set and configured to provide an alert, the terminal will send a notification to the user if the trailer crosses the geo-fence boundary. The geo-fence will send an alert when a trailer exits or enters the boundary through an email or pager notification. Geo-fences may also be removed or inactivated for trailers or groups of trailers at any time.

The UTT system will provide an on-board geo-fence with event-driven exception reporting. Exception-driven reporting will allow the UTT system to monitor trailer position and check for geo-fence breaks frequently, but send a message only if a geo-fence break is detected. Frequent checking for geo-fence breaks without sending frequent messages lowers messaging costs and increases battery life.

A geo-fence might be used to ensure that a trailer remained in a general area, such as the Los Angeles basin. In this example, the user would create a geo-fence around Los Angeles and then assign that geo-fence to a trailer or group of trailers. If a trailer was taken from the Los Angeles area, an alert would be generated and the user notified. This type of geo-fence might permanently remain in effect if this trailer or group of trailers were meant to stay in that area indefinitely. A geo-fence could also be created around a particular destination, such as a receiving warehouse. When the trailer entered this geo-fence, an alert would be generated so that the user would know that the trailer was delivered within a certain timeframe.

Using the UTT system, a user can set a self-centered geo-fence, which provides a quick way to set a geo-fence without forcing the user to locate the area on the map. A self-centered geo-fence uses the position of the trailer at the time of receiving the "set self-centered geo-fence" command to create the geo-fence boundary. The user does not have to create the geo-fence on a map or choose settings for that geo-fence. As with any geo-fence, an alert will notify the user if the trailer breaks the geo-fence boundary while the geo-fence is active.

All UTT system generated geo-fences shall have configurable start and end dates.

- The UTT system shall support a single geo-fence per trailer, which may be reset OTA.
- The UTT system terminal shall monitor the geo-fence at configurable intervals of 15 minutes; 1, 6, 8, 12, or 24 hours.

- The UTT system geo-fence monitoring interval shall default to once per hour.
- The UTT system geo-fence alert shall be configurable to be sent immediately upon validation, saved and sent with the next planned status message, or disabled.
- The UTT system geo-fences shall be configurable to generate an alert on exit, entry, or both.
- The UTT system software shall support the assignment and deletion of geo-fences to individual trailers.
- The UTT system software shall support the display of geo-fence summary data containing the trailer ID/SCAC; last known position; geo-fence status; last geo-fence alert message with location, door, cargo, and connect events; timestamps; and alert acknowledgement status.
- All UTT system geo-fence sizes shall be configurable.
- The UTT system shall support a self-centered geo-fence that is centered at the terminal location at time of receipt of the geo-fence command.
- The UTT system self-centered geo-fence default size shall be a square of 0.5 miles x 0.5 miles. (Note: 0.5 x 0.5 miles has been a useful setting in practice, but this setting and all other self-centered geo-fence default settings may be configurable by users. The UTT system in the pilot test allows the setting of a geo-fence as follows: East/West length from 500 to 40,000,000 meters and North/South Length from 500 to 20,000,000 meters.)
- The self-centered geo-fence default configuration shall be activated upon receipt by the UTT system terminal.
- The UTT system self-centered geo-fence default configuration shall remain active until deactivated by the user.
- The UTT system self-centered geo-fence default configuration shall be to send an alert when a trailer exits the geo-fence boundary.
- The UTT system self-centered geo-fence default configuration shall be to send alerts immediately, as opposed to saving alerts and sending them along with the next scheduled status message.
- The UTT system self-centered geo-fence default configuration settings shall be editable by system administrators.

4.2.1.5 Trailer cargo sensing

As a part of the UTT system, an ultrasonic sensor detects the presence of cargo in the trailer by indicating if the trailer is unloaded or loaded. A cargo "event" is defined as the transition from completely unloaded to partially or completely loaded or vice-versa. The UTT system terminal wakes up to check the cargo status at a predefined frequency, and a status message may be sent depending on user-chosen settings. For example, an erroneous detection could occur if a person walks into the trailer at the moment the sensor is taking a reading of cargo status. In this case, assuming the person exits the trailer, a second check would show the true unloaded state of the trailer. Validation of cargo events decreases the probability of erroneous state detections.

- The cargo sensor shall be configurable to monitor at four or more different frequencies, including once every 10, 30, 60, or 120 minutes.
- The cargo sensor shall be monitored at least once every 30 minutes by default.
- The cargo event message shall be configurable to be sent immediately upon validation, saved and sent with the next planned status message, or disabled.
- The cargo event message shall be sent immediately upon validation by default.
- The cargo sensor validation shall be configurable as follows: If a cargo state change is detected, the cargo sensor shall wait an interval of X minutes prior to rechecking, and shall recheck Y times, where X may be 5, 10, 30, or 120 minutes and Y may be 0, 1, 2, or 3.
- The cargo sensor default validation setting shall be to recheck one time (Y=1) after five minutes (X=5).
- The cargo event message shall include trailer position, if available. If the position is not available, the message shall provide the last known position with a timestamp or "position unknown".
- The cargo event status message shall include the last known cargo state (loaded or not loaded) and time of the last known cargo state.
- All of the above configurable parameters of the cargo sensor shall be OTA configurable by the user.

4.2.1.6 Trailer door sensing

As a part of the UTT system, the trailer door sensor monitors for an open or closed door on the trailer. A door event is defined as the transition from open to closed or from closed to open. The trailer door sensor can work in conjunction with the cargo sensor, so that only those door state changes that might affect cargo are sent to the user. For example, it is possible to configure the system to send door open events if there is cargo in the trailer and to ignore door open events if the trailer is empty.

For the pilot test, only trailers with a single set of doors will be monitored, and a door opening alert will only be sent when the trailer is loaded.

- The door sensor shall be configurable to trigger an event if the door goes from closed to open and remains open for a configurable amount of time, where the time may be 5, 10, or 30 seconds; or 1, 2, 3, 4, 5, 10, 30, or 60 minutes. 4
- The door sensor shall be configurable to trigger an event if the door goes from open to closed and remains closed for a configurable amount of time, where the time may be 30 seconds; 1, 10, 20, 30, or 60 minutes.
- The default configuration shall be not to send door closed events.
- The default configuration shall be to send an alert for door open events when the cargo sensor senses a loaded trailer.
- Door events shall be configurable to be sent immediately upon validation, saved and sent with the next planned status message, or disabled.
- Door event messages shall be sent immediately upon validation by default.
- The door event message shall include position, if available.
- The UTT system terminal shall automatically detect when a door sensor is installed.
- All of the above configurable parameters of the door sensor shall be OTA configurable by the user.

4.2.1.7 Alerts

Alerts are generated by the UTT system host software and presented to the viewer through an alert icon that is displayed near the trailer ID. Alerts are based on a combination of user-preferred settings and events which are generated from the mobile terminal. Alerts are used to notify the user of events, such as geo-fence violations. Alerts can be configured to be forwarded to email or pager addresses.

- UTT system alerts shall meet the requirements for the cargo sensor, trailer door sensor, and geo-fence as specified in each respective section above.
- UTT system alerts shall be configurable to be sent to a minimum of one email/pager address. (There is no requirement for a maximum number of addresses to which an alert may be forwarded.)
- The UTT system software shall allow a user to acknowledge alert messages and then the UTT system shall log the corresponding user ID.
- The UTT system software shall provide an optional alert for a trailer that has failed to send a scheduled status report for a period of X days, where X is configurable at any time.
- The UTT system software shall provide an optional alert for a trailer that has moved independently of its assigned tractor.
- The UTT system software shall provide an optional alert for a trailer that has been disconnected outside of a specified distance from any one of a list of user-specified drop points.
- The UTT system software shall provide an optional alert for a tractor that has sent a "load call" without being connected to a trailer. (A load call is a message sent from the tractor to a dispatcher indicating that it has connected to a trailer and is ready to depart.)
- The UTT system software shall provide an optional alert for a trailer that reports a door open event while the trailer is not empty.
- The UTT system software shall provide a way for the user to create and save an alert monitoring plan that may be assigned to trailers. (The purpose of this requirement is to help users specify alert settings quickly and easily for any trailer. Without a monitoring plan, the user would have to set each alert option)

4.4.4.8 Software requirements

Requirements for the software that is visible to the system user are included in this section. The UTT system-provider hosts this software that may be accessed by users through the Internet. Using the software, the user may

view information, such as trailer positions and cargo, door, geo-fence, or connection events, or configure settings for the system such as landmarks, trailer groups, and user accounts. Additional software requirements are listed in sections above describing time of trailer connection and disconnection, trailer location and mapping, geo-fencing, alerts, and incorporation of fleet management tools.

Messaging

- The UTT system software shall store in the database and display all incoming messages including trailer connect/disconnect, door open/closed, cargo empty/not empty, battery events, and status reports.
- The UTT system software shall support the configuration of terminal parameters by authorized users.
- The UTT system software shall support the ability for an authorized user to request an updated status report from the UTT system terminal.

Accounts

- The UTT system software shall support the administration of user accounts, including creation, modification, and deletion of accounts.
- The UTT system software shall allow authorized users from a user account to only access to their user account data.

User Interface

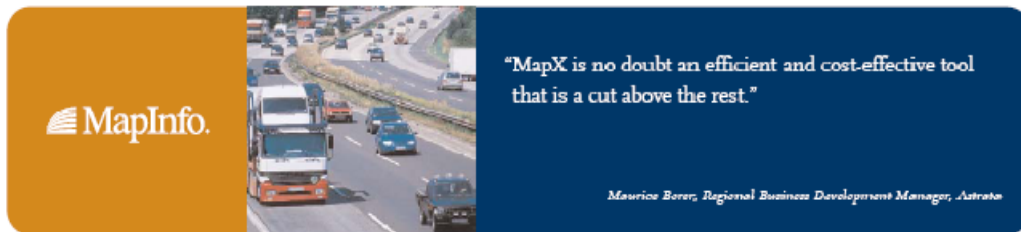
- The UTT system shall provide access to the data from an Internet browser.
- The UTT system shall support a password-protected secure log-in access to the user's account for authorized users.
- The UTT system software shall include a monitoring screen for the user to view all trailers, which will display the trailer ID, trailer type, terminal type, SCAC, date/time of last message, door status, connect status, cargo status, and last-known trailer location with proximity to city/town/landmark.
- The UTT system software shall allow authorized users to modify the labels of the sensors, such as the door sensor and cargo sensor.
- Using the UTT system software, authorized users shall be able to view and edit trailer details, including trailer ID, SCAC, trailer type, and description.
- Using the UTT system software, authorized users shall be able to view the event details and event history for a trailer including positions, cargo events, door events, and connect events for a user-selected time period (default to the prior week).
- Using the UTT system software, authorized users shall be able to view all messages including status reports, events, and positions for a given trailer in a time-sequential order for a user selected time period (default to the prior week).
- Using the UTT system software, authorized users shall be able to create and delete trailers and their history and to rename trailers (retaining history).

Appendix E

Singapore HazMat Transport Vehicle Tracking System

CASE STUDY: ASTRATA GROUP INCORPORATED

Astrata Group Incorporated Develops Anti-Terrorism Homeland Security Tracking and Control Solution for Singapore Government Using MapInfo's Mapping Technology.



CHALLENGE

The SCDF wanted to implement a system to carry out real-time tracking of vehicles carrying dangerous goods. This is to strengthen its ability to tackle unconventional chemical and biological threats as well as 'dirty' bombs i.e. any Radiological Dispersal Device, radiological weapon which combines radioactive material with conventional explosives.

SOLUTION

To meet the SCDF's requirements Astrata's Research and Development ("R&D") team for Homeland Security Products developed the Astrata Geo-Spatial Information Technology System (the "GEO-IT System"), an advanced tracking, monitoring, and control system.

After a rigorous evaluation exercise, MapInfo's MapX® software was chosen as the mapping technology for the HazMat Transport Vehicle Tracking System for the SCDF.

Astrata Group Incorporated (OTC Bulletin Board: ATG - News) is focused on advanced location-based IT services and solutions (GEO-IT) that combine GPS positioning, wireless communications (satellite or terrestrial) and geographical information technology, which together enable businesses and institutions to monitor, trace, or control the movement and status of machinery, vehicles, personnel and other remote assets. Astrata has designed, developed, manufactured and currently supports eight generations of GEO-IT systems with over 80,000 units deployed worldwide.

The intensification and proliferation of terrorist activities in the world has prompted the Singapore Government to step up its efforts to increase its homeland security. Companies such as Astrata Group Incorporated who develop advanced location-based IT services and solutions play an instrumental role in delivering homeland security tracking and control solutions to organisations and governments worldwide.

The Situation

The Singapore Civil Defence Force (SCDF) is charged with ensuring the safety of Singaporeans and the economy to near-normal conditions during any eventualities. Its main roles are to provide fire fighting, rescue and emergency ambulance services; as well as to formulate, implement and enforce regulations on fire safety and civil defence shelter matters.

One of the measures taken by the Singapore Civil Defence Force (SCDF) to address the threat of terrorism is to implement a system to carry out real-time tracking of vehicles carrying dangerous goods. This is to strengthen its ability to tackle unconventional chemical and

biological threats as well as 'dirty' bombs i.e. any Radiological Dispersal Device, radiological weapon which combines radioactive material with conventional explosives.

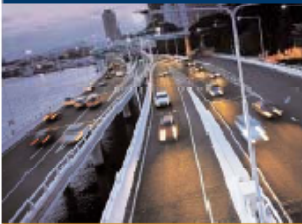
In September 2004, the SCDF invited several vendors to propose a vehicle tracking solution which could provide comprehensive tracking, monitoring, and sophisticated control functions. Following an intensive evaluation exercise of proposed solutions by vendors, Astrata (Singapore) Pte Ltd - a Joint Venture Company owned 51% by Astrata (Asia Pacific) Pte Ltd and 49% by PCS Security Pte Ltd - was awarded the contract to develop and implement a HazMat Transport Vehicle Tracking System (HTVTS).

To meet the SCDF's requirements Astrata's Research and Development ("R&D") team for Homeland Security Products developed the Astrata Geo-Spatial Information Technology System (the "GEO-IT System"), an advanced tracking, monitoring, and control system. Astrata's R&D team also embarked on a search for a superior mapping solution that could deliver the high performance required at a cost effective price. After a rigorous evaluation exercise, MapInfo's MapX® software was chosen as the mapping technology for the HazMat Transport Vehicle Tracking System for the SCDF.

The HazMat Transport Vehicle Tracking System (HTVTS) comprises two phases:

- Phase one involves the tracking of all local and foreign vehicles carrying bulk petroleum and toxic material
- Phase two involves the installation of an immobiliser which can remotely stop vehicles from entering exclusion zones.

THE MAPINFO ADVANTAGE



To meet SCDF's requirements for a HazMat Transport Vehicle Tracking System, Astrata developed the Geo-Spatial Information Technology System, an advanced tracking, monitoring, and control system incorporating MapInfo's mapping technology. MapInfo's MapX® mapping solution and engine was selected because it is proven, robust, flexible and easy to use. The ActiveX component enables Astrata's developers to add mapping functionalities to the application – seamlessly, quickly and easily. MapInfo's reliable and proven location intelligence technology complements and adds value to Astrata's product offerings by enabling Astrata to provide flexible and scalable solutions that can easily be customised to suit their customers' needs.

MapInfo Asia Pacific
Headquarters
L4 170 Pacific HWY
Greenwich, NSW Australia
T: +61 4 9437 4255
www.mapinfo.com.au

MapInfo Singapore
Representative Office
L30 Six Battery Road
Singapore 049909
T: +65 6322 0862
www.mapinfo.com.sg



"We are very pleased with the quality and performance of MapInfo's MapX and as such, we will continue to leverage on MapInfo's best of breed technology to develop innovative solutions for our customers"

Sandy Borthwick, Managing Director, Astrata, Asia Pacific Region

Using the solution developed by Astrata, the SCDF will be able to track all vehicles carrying hazardous materials and chemicals which could become a possible weapon used by terrorists. From the control room at their headquarters, SCDF officers will be able to monitor a vehicle's movement in real time and view the exact location and activities of each vehicle to prevent hazardous materials from being used as a weapon, as well as to minimise the impact of a possible terrorist attack using such materials.

Approximately 500 local HazMat transport vehicles will be fitted with a tracking device which is smaller than a mobile phone and fits under the dashboard. These vehicles can only travel along approved routes away from highly populated areas at specific times to reduce the impact of any possible disasters. If a vehicle strays from its path, the device will trigger an alarm, mobilising emergency services.

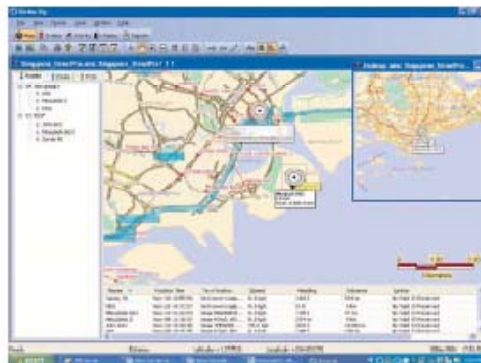
Another unique feature of this system is the ability to monitor vehicles in tunnels, urban canyons and underground parking structures. These capabilities set a new benchmark for security conscious nations around the world with similar concerns for public safety. At present, Singapore is the first country in the world to implement the HazMat transport vehicle tracking system.

The Benefits

Maurice Borer, Regional Business Development Manager, Astrata (Asia Pacific) said, "The choice was clear for our R&D team. They were looking for a mapping solution and engine which was proven, robust, flexible and easy to use. MapInfo's MapX® fulfilled all of these requirements. The ActiveX component enables our developers to add mapping functionalities to the application - seamlessly, quickly and easily. MapX is no doubt an efficient and cost-effective tool that is a cut above the rest."

MapInfo MapX helps simplify application development through its use of standard languages, a streamlined object model, extensive methods and events, efficient property pages, defaults and other wizards. It also offers users a highly visual way to display and analyse location-based data to better serve customers; and management to make better decisions and manage assets and operations more effectively.

Sandy Borthwick, Managing Director for Astrata's Asia Pacific Region, commented, "MapInfo's reliable and proven location intelligence technology complements and adds value to Astrata's product offerings by enabling us to provide flexible and scalable solutions that can easily be customised to suit our customers' needs. We are very pleased with the quality and performance of MapInfo's MapX and as such, we will continue to leverage on MapInfo's best of breed technology to develop innovative solutions for our customers."



Astrata's GEO-IT System is powered by MapInfo's MapX. The system monitors HazMat vehicles' movement in real time, allowing security personnel to view and track the exact location and activities of each vehicle from the control room.

APPENDIX F

Kentucky Hazmat Supply Chain Threat Analysis¹

What is the terrorist threat to the nation's hazmat supply chain?

The hazmat supply chain presents an attractive target for terrorists. In the United States, there are hundreds of thousands of shipments daily through a complicated supply chain with multiple points of vulnerability. Because of their nature, many hazmat shipments could become dangerous and ready-made weapons in the hands of a terrorist. And because of the large number of shipments, the exposure to these vulnerabilities is very broad.

Most hazmat shipments in the United States are by motor carriers, however hazardous materials are also shipped by rail and barge. Vulnerable points in the supply chain include manufacturing facilities, shippers, hazmat carriers, and receiving facilities.

A FMCSA study identified three terrorist attack profiles for hazmat shipments.²

1. **Theft** is undertaken by means of stealth, deception, or force. Stealth and deception are deterred by detection, while force assumes detection and operates within parameters defined by the time to communicate and mount an interdiction. Stealth, deception, and force also define an escalation path for operational planning purposes.
2. **Diversion** is a tactic that results in either theft or interception. The purpose is to create a path to a target opportunity or arrive at a location where control of the cargo by the terrorists can be achieved.
3. **Interception** is the "instantaneous" version of theft in that the cargo is released and/or detonated, and ignited while still in control of the shipper/carrier/consignee. Particularly effective when the radius of damage is large, this is potentially the most violent of attack profiles in that it likely involves explosives as the mechanism for effecting material release.

For example, for a bulk chemical shipment, a terrorist might use a false manifest to divert the chemical shipment for delivery to a populated area for intentional release.

Numerous international and domestic incidents have occurred over the past several years that demonstrate the threat posed to the hazmat supply chain by terrorists. For example, according to the FMCSA study the following events all occurred in a 2-month period in 2002:

- March 31, 2002: A 29-year-old driver for a propane distributor drove away with a 3,000-gallon bobtail. He made a telephone threat stating that he wanted to kill President George W. Bush and that he would use the bobtail as a "3,000-lb bomb".
- April 11, 2002: A terrorist driving a truck carrying liquefied natural gas ignited his cargo in front of a synagogue on the Tunisian Island of Djerba, killing 17 people, mainly German and French tourists. Al Qaeda claimed responsibility for the blast.
- May 16, 2002: A tractor-trailer carrying 10 tons of deadly cyanide in 96 drums was stolen after three armed men held up the vehicle north of Mexico City. Six drums were never found.

Hazardous materials are shipped by truck, rail, and barge – most by truck. The hazmat supply chain is vulnerable at a number of points.

The FMCSA has identified three terrorist attack profiles for hazmat shipments.

Terrorists have used hazmat shipments as weapons of mass destruction in incidents throughout the world.

¹ This analysis was prepared by **Brandon Montgomery** and **Matthew Tackett** – May 2008 – under the direction of Michael Barclay, Coldstream Digital LLC. Messrs. Montgomery and Tackett completed requirements for the Master of Public Administration degree from Morehead State University during the course of this project.

² Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis. 2004 pgs 51-52.

- May 2002: A fully loaded tanker truck pulled into Israel's largest fuel depot and suddenly caught fire due to an explosive charge connected to a cellular phone. The fire was extinguished, but had the truck exploded, destruction and death would have resulted.
- February 2007: Insurgents in Iraq incorporated canisters of liquefied chlorine into vehicle-borne improvised explosive devices. The blast left several dead and scores suffering from exposure to the dispersed chlorine in an area of Baghdad.
- April 2007: A suicide truck bomb loaded with chlorine gas exploded in Ramadi killing as many as 30 people, many of them children, a security official said. The truck, a fuel tanker loaded with the toxic gas, struck in the late morning of the Muslim day of prayer when children off from school usually play in the street and adults run errands and visit before going to the mosque at midday.

What are the potential costs of a hazmat attack?

The consequences of an attack using hazardous materials could be significant. A FMCSA study explored the "per event" potential economic impact of intentional and non-intentional releases of hazardous materials.³ The study examined the potential consequences as measured by the following parameters.

- Fatalities and injuries.
- Property Damage: Damage to the truck, to other involved vehicles, and to other public and private property.
- Product Loss: Quantity and value of the hazardous materials lost during a spill.
- Environmental damage.
- Evacuation: Predominantly short-term relocation of people and business operations.
- Cleanup: Stopping the spread of a release and removing spilled materials.
- Traffic Delay: Additional travel time experienced by the motoring public due to delays caused by the incident.
- Business Disruption: Businesses having to reduce or cease operations because the facility is inaccessible, supplies cannot be received, or other constraints imposed by the incident.

The study presented the following estimates of the economic consequences of a terrorist attack using different types of hazmat shipments.

Figure 1. Estimated economic consequence of terrorist attacks.

Hazardous Material Load Type	Reasonable Worst-Case Hazmat Attack Consequences
Bulk Fuel	\$3.7 Billion
Less Than Load High Hazard	\$2.1 Billion
Bulk Chemicals	\$16.3 Billion
Truckload Explosives	\$13.3 Billion

To put the FMCSA numbers into context, the economic consequences of two terrorist attacks in the U.S. - the 1993 New York World Trade Center (WTC) and the 1995 Oklahoma City Federal Building - can be examined.

A terrorist attack using a hazmat shipment as a weapon of mass destruction can cause huge economic disruptions.

The FMCSA estimates a single hazmat attack can create economic damages of more than \$16 Billion.

³ Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis. 2004 pgs 70-71

- The 1993 WTC bombing killed six people, injured over 1,000, and resulted in over \$113 million in loss of life and bodily injury, and over \$510 million in insured losses (based on figures from the Federal Emergency Management Agency). Total losses are estimated to be \$623 million.
- The Oklahoma City bombing killed 168 people, injured 601, and resulted in \$560 million in loss of life and bodily injury, and over \$125 million in insured losses. Total losses are estimated to be \$685 million.

Vehicles used in the transportation of hazardous materials typically have much larger capacities than the vehicles used in these two incidents. If larger vehicles were used to carry out a terrorist act, the damage would have been far worse. If highly hazardous materials were involved and released in a directed attack, it could result in far greater numbers of casualties and damage to property over a larger area.

Another example of the economic consequence of directed attacks in the United States, albeit attack(s) using airplanes against buildings as opposed to trucks, is the September 11, 2001 attack(s) on the WTC. According to the FMCSA, the Government Accounting Office (GAO) reviewed eight studies from seven organizations that examined the financial impacts of the 9-11 attack on the World Trade Center. The GAO concluded that the study conducted by the New York City Partnership and Chamber of Commerce provided the most comprehensive estimates: \$83 billion in 2001 dollars for direct and indirect costs.

The attack on the World Trade Towers on 9/11 cost more than \$80 Billion.

What is being done to protect the nation's hazmat supply chain?

The federal government has undertaken a number of initiatives focused on the security of the hazmat supply chain. Federal initiatives include the following.

1. **U.S. Transportation Security Administration hazmat driver security checks.** Under the USA Patriot Act, the U.S. Transportation Security Administration (TSA) has issued rules that prohibit states from issuing a hazardous materials endorsement to a trucker without first determining whether or not the individual poses a security risk. The laws's intent is to prevent hazmat shipments from falling into the hands of individuals that might use them as weapons.
2. **U.S. Federal Motor Carrier Safety Administration hazardous materials safety permits.** On June 30, 2004, the U.S. FMCSA issued a rule to establish a national safety permit program for motor carriers that transport certain hazardous materials in interstate or intrastate commerce. FMCSA's hazmat permitting requirements began a staged phase-in beginning January 1, 2005. A motor carrier must meet three minimal requirements to obtain a hazmat safety permit.
 - o **Satisfactory safety rating.** The motor carrier must have a "satisfactory" safety rating assigned by either FMCSA, pursuant to the Safety Fitness Procedures of part 385 of this subchapter, or the State in which the motor carrier has its principal place of business, if the State has adopted and implemented safety fitness procedures that are equivalent to the procedures in subpart A of part 385 of this subchapter.
 - o **Satisfactory security program.** The motor carrier must establish that it has a satisfactory security program, including:
 - A security plan meeting the requirements of part 172, subpart I of this title. The security plan must address how the carrier will ensure the security of the written route plan required by this part;
 - A communications system installed on each motor vehicle used to transport a hazardous material listed in Sec. 385.403(a) of this subpart that enables the vehicle operator to immediately contact the motor carrier during the course of transportation of the hazardous material, and each operator must be trained in the use of the communications system; and Hazmat employees who have all successfully completed the security training required in Sec. 172.704(a)(4) of 49 CFR.
 - o **Registration with RSPA.** The motor carrier must be registered with RSPA in accordance with subpart G of part 107 of 49 CFR.
3. **H.R. 1: Implementing Recommendations of the 9/11 Commission Act of 2007.** Section 1554 of the act directs the Secretary, through the TSA Administrator,

Hazmat carriers have to meet minimal requirements to obtain hazmat safety permits including a satisfactory security program.

to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials and to equip vehicles used in such shipments with technology that provides frequent or continuous communications, vehicle position location and tracking capabilities, and a feature that allows the driver to broadcast an emergency distress signal.

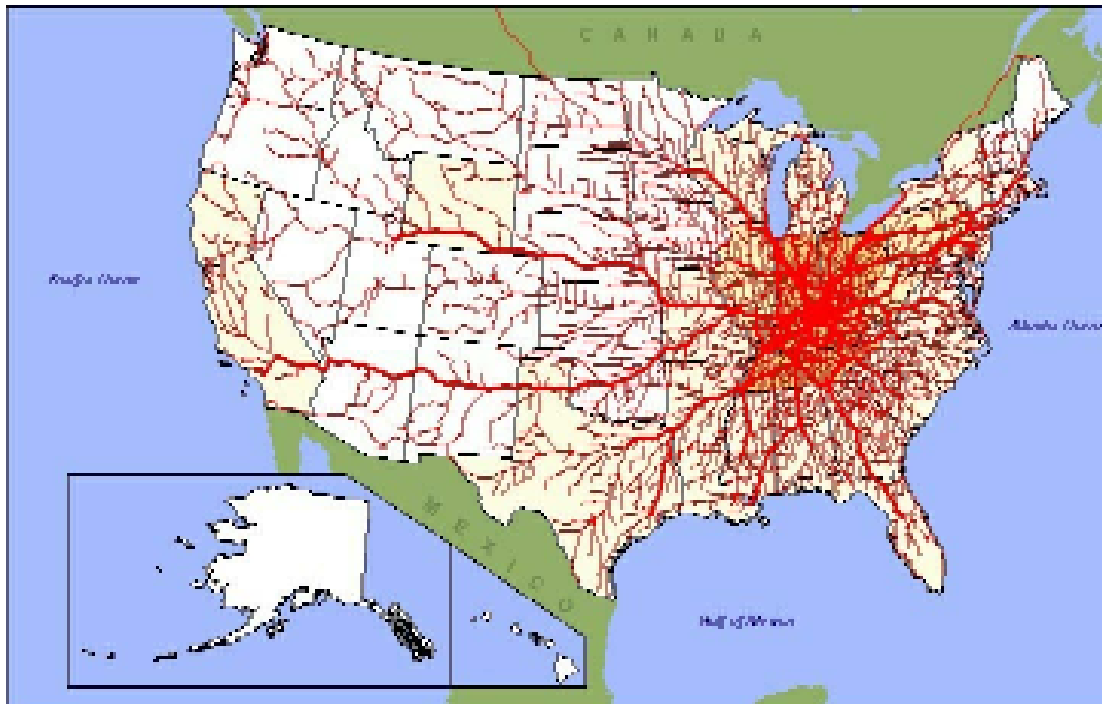
How is Kentucky's hazmat supply chain structured?

Kentucky is a key transit state for the interstate movement of hazardous materials by truck, barge, and rail.

Kentucky sits in the middle of one of the nation's busiest transportation corridors. Major interstate highways including I-64, I-65, and I-75 cut through the state carrying over 70,000 semi-tractor trailer trucks daily. The Ohio River and the Mississippi River border Kentucky and carry much of the nation's barge traffic. In addition, several major rail lines including CSX and Norfolk Southern have major rail lines through the state and hazmat shipments are regularly routed through the middle of Kentucky's urban areas. In Lexington, for example, 30 railcars a day carry hazardous materials through the heart of the city.⁴

U.S. Department of Transportation data on state truck tonnage indicates that only six states have more truck tonnage than Kentucky. DOT data also indicates that about 60% of the truck tonnage on Kentucky's roads is through traffic – a relatively high percentage. **Figure 2** illustrates freight flows to, from and within Kentucky.

Figure 2. Freight flows to, from, and within Kentucky by truck (Federal Highway Administration)



Kentucky produces (or stores) a significant amount of hazardous materials that could be used as weapons of mass destruction.

Kentucky has a number of facilities that produce or store significant amounts of hazardous materials. These include petrochemical facilities in western Kentucky, eastern Kentucky, and Louisville. In addition to its petrochemical facilities, Kentucky is also home to the Bluegrass Army Depot near Richmond and the Paducah Gaseous Diffusion Plant. The Bluegrass Army Depot is a repository for nerve agents. The Paducah Diffusion Plant produces low-enriched uranium fuel for commercial nuclear power plants.

⁴ "Hazmat Spills 'Significant Risk,' Officials Says", February 20, 2007
<http://www.redorbit.com/news/display/?id=846932>

How likely is it that groups residing in Kentucky have the means and organizational skill to launch an attack on the hazmat supply chain?

A major terrorist action involving hazardous materials in Kentucky will take considerable organizational skill and funding. As noted above, Kentucky does not have a large foreign-born population, and it is unlikely that a significant number of well-organized and well-funded “terrorist cells” reside within the state.

The threat of domestic terrorism is also low. There are domestic groups or individuals of concern in the state but none are likely to be organized well enough or suitably funded to initiate an action of concern.

A terrorist action in Kentucky involving hazardous materials would probably be carried out by groups residing outside the state.

Should Kentucky officials be concerned about threats to its hazmat supply chain?

Even though Kentucky might not be home to domestic or foreign-born terrorist groups that have the means and organizational skill to launch an attack on the hazmat supply chain, there are still significant threats to the hazmat supply chain in Kentucky.

Kentucky is a major transit state for hazmat shipments. A huge amount of goods pass through Kentucky on its interstate highway system. Barges hauling hazardous materials travel past major port cities on the Ohio River and the Mississippi River and trains transporting hazardous materials pass through all of Kentucky’s major metropolitan areas. Also, a significant amount of dangerous hazardous materials are produced or stored in Kentucky.

Kentucky is a “magnet” for terrorists seeking to attack the hazmat supply chain.

In Kentucky’s case, terrorist groups that are intent on attacking the hazmat supply chain are likely to come into Kentucky from out of state. In fact, Kentucky might well be a “magnet” for out-of-state terrorists seeking to launch attacks using hazardous materials. As noted previously, an attack on the hazmat supply chain could come about by theft, diversion, or interception. The hazmat attack scenarios listed below serve as examples of the potential attractiveness of Kentucky’s hazmat supply chain to terrorists.

1. Petrochemical facilities in the state represent an attractive target for terrorists either as a source of materials for use as a weapon of mass destruction or as a fixed target (i.e. destruction in place).
2. The Bluegrass Army Depot and the Paducah Gaseous Diffusion Plant produce or store hazardous materials that could serve as exceptionally dangerous weapons of mass destruction.
3. Kentucky is home to major tourist and sporting venues that draw huge numbers of people (see **Figure 3**). These venues are potentially attractive targets for terrorists using hazardous materials as weapons of mass destruction.
4. Numerous hazmat shipments travel daily by rail through the heart of Kentucky’s largest cities. Terrorists could intercept tank cars and release of their contents in crowded urban areas.
5. Terrorists could intercept barges hauling hazmat shipments on the Ohio River and the Mississippi River and release their contents in crowded urban areas or use the barge and its contents as a floating bomb.
6. Kentucky’s interstate road system might also serve as a magnet for terrorists. Hazmat shipments traveling on the Kentucky’s roads could be intercepted and used by terrorists. In addition, Kentucky’s interstate road system offers terrorists an efficient transportation route for moving dangerous materials through Kentucky to high value targets in the Northeast, Southeast or Midwest. ⁵

Hazardous materials in Kentucky are vulnerable to theft, diversion, or interception.

Figure 4 further describes each of the six attack scenarios listed above.

Figure 3. Kentucky is home to major sporting and tourist events.

⁵ For example, concern that Kentucky’s interstate road system might be used as the delivery route for radioactive WMDs led the Kentucky Transportation Cabinet and the U.S. Department of Homeland Security to install radiation detectors at a number of truck weigh stations on Kentucky’s interstate highway system.

Events	Event Date	Location	Est. Attendance
Kentucky Derby (race day – Churchill Downs)	May	Louisville, JEFFERSON	160,000
Thunder Over Louisville	April	Louisville, JEFFERSON	800,000
Kentucky Oaks Horse Race	April	Louisville, JEFFERSON	110,000
Keeneland Track Spring/Fall Meet	April/October	Lexington, FAYETTE	15,000
Churchill Downs Spring/Fall Meet	April –July October-November	Louisville, JEFFERSON	15,000
University of Kentucky Football Games	August - December	Lexington, FAYETTE	70,000
University of Kentucky Basketball Games	November - March	Lexington, FAYETTE	25,000
University of Louisville Football Games	August - December	Louisville, JEFFERSON	45,000
University of Louisville Basketball Games	November - March	Louisville, JEFFERSON	19,000
Meijer 300 NASCAR Race	6/14/2008	Sparta, GALLATIN	66,000
Meijer Indy 300 Race	8/9/2008	Sparta, GALLATIN	66,000
PGA's Ryder Cup Golf Tournament	9/16-9/21, 2008	Louisville, JEFFERSON	240,000
Alltech FEI World Equestrian Games	9/25 – 10/10, 2010	Lexington, FAYETTE	800,000

Figure 4. Hazmat Attack Scenarios in Kentucky

Scenarios	Target	Means	Impacts
Theft or diversion of bulk chemical shipment from Kentucky-based petrochemical plant.	Major metropolitan area or major tourist or sports event.	Theft or diversion of hazmat truck shipment. Release and/or detonation of truck contents.	Fatalities and injuries.
Destruction of hazardous materials on-site at fixed facilities.	Petrochemical plants in Louisville, eastern Kentucky, or western Kentucky.	Theft, release or detonation of hazardous materials found on site.	Fatalities and injuries. Significant damage to infrastructure.
Theft (by force) of nerve agents (Bluegrass Depot) or radioactive materials (Paducah).	Major metropolitan area or major tourist or sports event.	Theft of agents on site, or hijacking of from hazmat carrier.	Fatalities and injuries.
Interception of train hauling hazardous materials.	Major metropolitan area or target of interest adjacent to railway.	Hijacking of train while en route to destination.	Fatalities and injuries.
Interception of barge hauling hazardous materials.	Metropolitan river ports on Ohio River or strategic infrastructure (bridges, locks).	Hijacking of barge while en route to destination.	Fatalities and injuries. Destruction of ports or strategic infrastructure.
Attack of major tourist or sporting venues using hazardous materials as WMD.	Heavily populated events, such as those indicated in Figure 1.3.	Release or detonation of stolen hazardous material.	Fatalities and injuries. Disruption of high profile event.
Transport of radioactive materials through Kentucky by truck.	Kentucky's Interstate and Highway System	Relaying hijacked material through Kentucky.	Unmonitored and dangerous transportation.

• • •

Appendix G

Kentucky Revised Statutes Hazardous Materials

<http://www.lrc.ky.gov/krs/titles.htm>

174.400 Legislative intent.

Due to the central geographical location of the Commonwealth with respect to the hazardous materials industry, and since most predictions indicate that the amount of hazardous material in transport should substantially increase in the future, it is the intent of KRS 174.405 to 174.425 to provide for the public health and safety of the citizens and to protect the environment of the Commonwealth when any hazardous material is being transported within, or, in the case of radioactive materials, within or through this state.

Effective: July 15, 1994

History: Amended 1994 Ky. Acts ch. 99, sec. 2, effective July 15, 1994. – Created 1980 Ky. Acts ch. 384, sec. 1, effective July 15, 1980.

174.410 Administrative regulations and agreements with other cabinets.

(1) The secretary shall be responsible for controlling and regulating the movement of all radioactive materials and the intrastate transport of other hazardous materials transported by all carrier modes within the Commonwealth.

(2) The secretary, in consultation with the secretary of the Environmental and Public Protection Cabinet and the secretary of the Cabinet for Health and Family Services, shall adopt by reference or in entirety, the Federal Hazardous Materials Transportation Regulations, 49 C.F.R. (1978), as amended, to effectively carry out the intent of KRS 174.400 to 174.425.

(3) The cabinet and the Justice Cabinet shall cooperate with and assist the Environmental and Public Protection Cabinet in implementing and enforcing the transportation provisions of any state hazardous waste regulations promulgated pursuant to KRS Chapter 224. The specific nature and details of the assistance effort shall be established by a formal cooperative agreement acceptable to the cabinets, and all activities shall occur in accordance with the terms of the agreement. The agreement shall address and include, but not necessarily be limited to, the following items:

(a) As a part of routine and periodic transportation checks and inspections, ensure that shipments of hazardous waste do not present a threat to the public or the environment; are accompanied by the required hazardous waste manifest or such other shipping or delivery documents as may be acceptable to the Environmental and Public Protection Cabinet; and comply with applicable shipping standards;

(b) Upon receipt of a written request from the secretary or general counsel of the Environmental and Public Protection Cabinet, actively conduct field investigations relating to the illegal, improper, or unauthorized transport of hazardous waste in the state. Such investigations may, at a minimum, include passive and active surveillance, apprehension, and reporting, with the scope and extent of each investigation to be previously agreed to by the involved cabinets;

(c) Compile and maintain such necessary records that may normally be required to carry out the provisions of this subsection and shall for minor violations report quarterly, and for major violations report weekly, to the Environmental and Public Protection Cabinet on the status of the interagency hazardous waste transportation monitoring and enforcement activity for irregularities or violations;

(d) Provide any information, evidence, and other support, either in written form or in the form of oral testimony during a legal proceeding or both, as may be required by the Environmental and Public Protection Cabinet to fully carry out its statutory responsibility under the appropriate sections of KRS Chapter 224;

(e) The Environmental and Public Protection Cabinet shall, unless specifically agreed otherwise, have primary responsibility for initiating and conducting all legal proceedings arising from the terms and provisions of this subsection; and

(f) The Environmental and Public Protection Cabinet shall provide sufficient training, technical assistance, and other support to the appropriate cabinets to prepare representatives of the cabinets to adequately carry out the responsibilities set forth in this subsection.

Effective: June 20, 2005

History: Amended 2005 Ky. Acts ch. 99, sec. 142, effective June 20, 2005. – Amended 1998 Ky. Acts ch. 426, sec. 121, effective July 15, 1998. -- Amended 1994 Ky. Acts ch. 99, sec. 4, effective July 15, 1994. -- Created 1980 Ky. Acts ch. 484, sec. 3, effective July 15, 1980.

Legislative Research Commission Note (6/20/2005). 2005 Ky. Acts chs. 11, 85, 95, 97, 98, 99, 123, and 181 instruct the Reviser of Statutes to correct statutory references to agencies and officers whose names have been changed in 2005 legislation confirming the reorganization of the executive branch. Such a correction has been made in this section.

174.415 Inspection and enforcement program.

The secretary shall establish an inspection and enforcement program to determine compliance with the provisions of KRS 174.400 to 174.425, and any regulations promulgated under KRS 174.410. In carrying out the provisions of KRS 174.400 to 174.425, the secretary shall not duplicate the enforcement and inspection activities performed by the federal government.

Effective: July 15, 1994

History: Amended 1994 Ky. Acts ch. 99, sec. 5, effective July 15, 1994. -- Created 1980 Ky. Acts ch. 384, sec. 4, effective July 15, 1980.

174.420 Carrying of shipping papers and hazardous waste manifest.

(1) Any person transporting hazardous materials in the Commonwealth shall carry a copy of the shipping papers required in 49 C.F.R. (1978), as amended, in the transporting vehicle while in the Commonwealth.

(2) In the event of an accident involving hazardous material, the operator of the vehicle shall:

(a) Notify the Kentucky State Police of the accident within one (1) hour, who shall then notify the local jurisdiction and any other appropriate state agency with emergency action responsibility, and

(b) Provide the shipping papers to state and local emergency response authorities, and immediately bring to their attention the fact that the vehicle is transporting hazardous materials.

(3) In addition to the other requirements of this section, any person transporting hazardous wastes shall carry in the transporting vehicle a copy of a manifest in a form approved by the Environmental and Public Protection Cabinet.

Effective: July 15, 1994

History: Amended 1994 Ky. Acts ch. 99, sec. 7, effective July 15, 1994. -- Created 1980 Ky. Acts ch. 384, sec. 5, effective July 15, 1980.

Legislative Research Commission Note (6/20/2005). 2005 Ky. Acts chs. 11, 85, 95, 97, 98, 99, 123, and 181 instruct the Reviser of Statutes to correct statutory references to agencies and officers whose names have been changed in 2005 legislation confirming the reorganization of the executive branch. Such a correction has been made in this section.

**Kentucky Revised Statutes
Hazardous Wastes**

<http://www.lrc.ky.gov/krs/titles.htm>

224.46-012 Registration fee for generator of hazardous waste.

(1) A generator of hazardous waste required by KRS Chapter 224 to register with the cabinet shall be subject to an annual registration fee by the cabinet and the fee shall be equal to the cost of review but shall not exceed the following amounts:

(a) For one (1) to five (5) waste streams: three hundred dollars (\$300);

(b) For six (6) to ten (10) waste streams: three hundred fifty dollars (\$350);

(c) For eleven (11) to fifteen (15) waste streams: four hundred dollars (\$400);

(d) For sixteen (16) to twenty (20) waste streams: four hundred fifty dollars (\$450);

(e) For twenty-one (21) to twenty-five (25) waste streams: five hundred dollars (\$500);

(f) For twenty-six (26) to thirty (30) waste streams: five hundred fifty dollars (\$550); and

(g) For thirty-one (31) or more waste streams: six hundred dollars (\$600).

(2) If a generator of hazardous waste submits to the cabinet a registration to modify waste streams, the following fees shall be imposed:

(a) For one (1) to five (5) waste streams: fifty dollars (\$50);

(b) For six (6) to ten (10) waste streams: one hundred dollars (\$100);

(c) For eleven (11) to fifteen (15) waste streams: one hundred fifty dollars (\$150);

(d) For sixteen (16) to twenty (20) waste streams: two hundred dollars (\$200);

(e) For twenty-one (21) to twenty-five (25) waste streams: two hundred fifty dollars (\$250);

(f) For twenty-six (26) to thirty (30) waste streams: three hundred dollars (\$300); and

(g) For thirty-one (31) or more waste streams: three hundred fifty dollars (\$350).

(3) If a generator of hazardous waste submits to the cabinet a registration to modify any information other than its waste streams, it shall be subject to a fee by the cabinet of fifty dollars (\$50).

(4) The cabinet shall not impose a fee if a generator of hazardous waste modifies a registration by making a name change.

Effective: July 13, 1990

History: Created 1990 Ky. Acts ch. 471, sec. 2, effective July 13, 1990.

Formerly codified as KRS 224.1155.

224.46-560 Standards relating to transporters -- Agency cooperation.

The cabinet shall promulgate regulations establishing standards applicable to transporters of hazardous waste regarding record keeping, notification and compliance with the manifest system. The Transportation Cabinet and the Justice Cabinet shall cooperate with and assist the cabinet in implementing and enforcing the transportation provisions of any state hazardous waste regulations promulgated pursuant to this chapter. The specific nature and details of the assistance effort shall be established by a formal cooperative agreement acceptable to the cabinets.

Effective: July 15, 1986

History: Amended 1986 Ky. Acts ch. 237, sec. 4, effective July 15, 1986. – Created 1980 Ky. Acts ch. 264, sec. 10, effective July 15, 1980.

Formerly codified as KRS 224.873.

Legislative Research Commission Note. Acts 1986, ch. 237, § 9, provides: "The regulations promulgated under the introductory paragraph of subsection (1) of KRS 224.46-510 and under KRS 224.46-560, pursuant to the authority granted by sections 2 and 4 of this Act shall be no more stringent than the federal requirements."

224.46-570 Manifest system.

The cabinet shall require the use of a manifest system for the orderly tracking of hazardous wastes from the generation site to the site of treatment, storage, and disposal except for coal mining wastes pursuant to KRS 224.50-760(1)(c). The system shall, at a minimum, require the designation of the generator, each transporter, the disposal facility, and the type and quantity of waste involved. The cabinet may establish additional criteria to accommodate the manifest system to internal record keeping and to facilitate the monitoring of hazardous waste activity within the Commonwealth.

Effective: July 15, 1980

History: Created 1980 Ky. Acts ch. 264, sec. 9, effective July 15, 1980.

Formerly codified as KRS 224.874.

224.46-580 Development of statewide programs -- Responsibilities of cabinet -- Hazardous waste assessment -- Hazardous waste management fund -- Pollution prevention fund -- Response actions to release of waste -- Post-closure site integrity.

(1) The General Assembly declares that it is the purpose of this section to promote the development of statewide programs, under the responsibility of a single agency, which are intended to protect the health of the citizens and the environment of the Commonwealth from present and future threats associated with the management of hazardous wastes and the release of toxic chemicals regulated under Title III, Section 313 of the Superfund Amendments and Reauthorization Act of 1986, including disposal, treatment, recycling, storage, and transportation. The intent of the General Assembly is to add to and coordinate, and not replace, existing efforts and responsibilities in the areas of hazardous waste management, toxic chemical manufacture, processing, or other use, and to leave the primary burden and responsibility for hazardous waste and toxic chemical reduction on private industry; and further to finance assistance and coordination by imposing assessments on the generation of hazardous waste. The assessments are intended to produce a reduction in waste generated; to promote the use of new techniques in recycling, treatment, and alternatives other than land disposal; and to place the burden of financing additional hazardous waste management activities necessarily undertaken by state agencies on the users of those products associated with the generation of hazardous waste. The General Assembly further finds that Kentucky's industries need assistance in developing and implementing pollution prevention goals and that a fund should be established to provide technical and financial assistance to those industries.

(2) The Environmental and Public Protection Cabinet is given the authority to administer the provisions and programs of this section and the responsibility to achieve the purposes of this section.

(3) In addition to all specific responsibilities contained elsewhere in this chapter, the cabinet shall:

(a) Respond effectively and in a timely manner to emergencies created by the release of hazardous substances, as defined in KRS 224.01-400, into the environment. The cabinet shall provide for adequate containment and removal of the hazardous substances in order that the threat of a release or actual release of the substance may be abated and resultant harm to the environment minimized. The provisions of KRS 45A.695 to 45A.725 may be suspended by the cabinet if necessary to respond to an environmental emergency.

(b) Provide for post-closure monitoring and maintenance of hazardous waste disposal sites upon termination of post-closure monitoring and maintenance responsibilities by persons permitted to operate the facility pursuant to this chapter.

(c) Identify, investigate, classify, contain, or clean up any release, threatened release, or disposal of a hazardous substance where responsible parties are economically or otherwise unavailable to properly address the problem and the problem represents an imminent danger to the health of the citizens and the environment of the Commonwealth.

(4) The cabinet shall have the authority to finance the nonfederal share of the cost for clean up of sites under the Comprehensive Environmental Response, Compensation and Liability Act of 1980 (Pub. L. 96-510).

(5) The cabinet shall recover, when possible, actual and necessary expenditures incurred in carrying out the duties under this section. Any expenditures recovered shall be placed in the hazardous waste management fund.

(6) It is the expressed purpose of this section to accomplish effective hazardous waste and toxic chemical management that results in a reduction of the generation of hazardous wastes and the release of toxic chemicals within the Commonwealth; further, it is a purpose of this chapter to allocate a portion of the cost of administering necessary governmental programs related to hazardous waste and toxic chemical management to those industries whose products are reasonably related to the generation of hazardous waste.

(7) There is hereby imposed upon every person engaged within this state in the generation of hazardous waste an annual hazardous waste assessment to be determined pursuant to this section according to the quantity by weight of hazardous waste generated, except that no assessment shall be levied against generators for any quantity of "special wastes," waste oil, or spent material from air pollution control devices controlling emissions from coke manufacturing facilities. The assessment shall not be imposed upon any person for any quantities of hazardous waste generated by others for which that person is a secondary handler that stores, processes, or reclaims the waste. The assessment shall be reported and paid to the Environmental and Public Protection Cabinet for the generation of hazardous waste on an annual basis on January 1 of each year. The payment shall be accompanied by a report or return in a form that the cabinet may prescribe. If a federal law is enacted which accomplishes or purports to accomplish the purposes set forth in this section and which levies an assessment or tax upon any business assessed pursuant to this section, the amount of the assessment to be levied upon the business under this section shall be reduced by the amount of the federal assessment or tax upon the business. The reduction shall only be authorized when funds raised by the federal assessment or tax are made available to the state for any of the activities to be funded under this section. If federal moneys are available to carry out the duties imposed by subsection (3) of this section, the assessment shall cease to be levied and collected until such time as federal moneys are no longer available to the Commonwealth for these purposes. The assessment shall be charged against generators of hazardous waste until June 30, 2006. After this date, no further hazardous waste management assessment shall be charged against generators.

(8) The assessment on generators shall be one and two-tenths cents (\$0.012) per pound if the waste is liquid, or two-tenths of a cent (\$0.002) per pound if the waste is solid.

(a) Hazardous waste that is injected into a permitted underground injection well shall be assessed on a dry weight basis;

(b) Hazardous waste treated, detoxified, solidified, neutralized, recycled, incinerated, or disposed of on-site shall be assessed at one-half (1/2) of the appropriate rate, except for recycled waste used in the steel manufacturing process which shall be exempt;

(c) Waste that is subject to regulation under Section 402 or 307B of the Federal Clean Water Act shall be exempt; and

(d) Emission control dust and sludge from the primary production of steel that is recycled by high temperature metals recovery or managed by stabilization of metals shall be exempt.

(9) Except for waste brought into the state by a company to an affiliated manufacturing facility of the company receiving the waste, any person who transports hazardous waste into the state for land disposal or treatment which is generated outside of the state shall pay an assessment to the hazardous waste facility which first receives the waste for storage, treatment, or land disposal. The assessment rate shall be identical to the rate described in subsection (8) of this section. The facility shall remit the assessment to the cabinet on an annual basis on January 1 of each year. The payment shall be accompanied by a return the cabinet shall prescribe.

(10) If any generator or hazardous waste facility subject to the provisions of subsection (8) or (9) of this section fails or refuses to file a return or furnish any information requested in writing by the cabinet, the cabinet may, from any information in its possession, make an estimate and issue an assessment against the generator or hazardous waste facility and add a penalty of ten percent (10%) of the amount of the assessment so determined. This penalty shall be in addition to all other applicable penalties in this chapter.

(11) If any generator or hazardous waste facility subject to the provisions of subsection (8) or (9) of this section fails to make and file a return required by this chapter on or before the due date of the return or the due date as extended by the cabinet, unless it is shown to the satisfaction of the cabinet, that the failure is due to reasonable cause, five percent (5%) of the assessment found to be due by the cabinet shall be added to the assessment for

each thirty (30) days or fraction thereof elapsing between the due date of the return and the date on which it is filed, but the total penalty shall not exceed twenty-five percent (25%) of the assessment.

(12) If the assessment imposed by this chapter, whether assessed by the cabinet, or the generator, or any installment or portion of the assessment is not paid on or before the date prescribed for its payment, there shall be collected, as a part of the assessment, interest upon the unpaid amount at the rate of eight percent (8%) per annum from the date prescribed for its payment until payment is actually made to the cabinet.

(13) There is hereby created within the State Treasury a trust and agency fund which shall not lapse to be known as the hazardous waste management fund. The fund shall be deposited in an interest-bearing account. The cabinet shall be responsible for collecting and receiving funds as provided in this section, and all such assessments collected or received by the State Treasury shall be deposited in the hazardous waste management fund. All interest earned on the money deposited in the fund shall be deposited to the fund. When the State Treasurer certifies to the cabinet that the uncommitted balance of the hazardous waste management fund exceeds six million dollars (\$6,000,000), assessments shall not be collected until the State Treasurer certifies to the cabinet that the balance in the hazardous waste management fund is less than three million dollars (\$3,000,000). The implementation of the cap on the fund shall be suspended from July 13, 1990, until July 1, 1991. In addition, for assessments paid after July 1, 1991, the cabinet shall refund or grant a credit against the next assessment to come due, on a pro-rated basis, any money collected in one (1) year in excess of the cap.

(14) There is hereby created within the State Treasury a trust and agency account which shall not lapse to be known as the pollution prevention fund. The fund shall be placed in an interest-bearing account. The fund shall be administered by the Center for Pollution Prevention. The cabinet shall remit to the fund each fiscal year twenty percent (20%) of the funds received by the hazardous waste management fund subject to the enacted budget bill. The cabinet shall provide to the center estimates of the amount of the hazardous waste assessment expected to be collected during each upcoming fiscal year.

(15) Upon request of the secretary, moneys accumulated in the hazardous waste management fund shall be released in amounts necessary to accomplish the performance of the duties imposed by subsection (3) of this section. However, moneys from the fund shall not be used when federal moneys are available to carry out these duties, except when immediate action is required to protect public health or the environment, in which case the cabinet shall actively pursue reimbursement of the fund by any available federal moneys.

(16) If any person responsible for a release or threatened release of a hazardous substance fails to take response actions or to make reasonable progress in completing response actions ordered by the cabinet, the cabinet may bring an action to compel performance or may take appropriate response actions and order the responsible person to reimburse the cabinet for the actual costs incurred by the cabinet.

(17) If disposal activities have occurred at a hazardous waste site, the cabinet shall record in the office of the county clerk in the county in which a waste site is situated a notice containing a legal description of the property that discloses to any potential transferee that the land was used to dispose hazardous waste and that further information on the hazardous waste site may be obtained from the cabinet.

(18) No person shall affect the integrity of the final cover, liners, or any other components of any containment system after closure of a hazardous waste site on or in which hazardous waste remains without prior written approval of the cabinet.

Effective: July 13, 2004

History: Amended 2004 Ky. Acts ch. 44, sec. 1, effective July 13, 2004. -- Amended 2002 Ky. Acts ch. 54, sec. 1, effective July 15, 2002. -- Amended 2000 Ky. Acts ch. 351, sec. 1, effective July 14, 2000. -- Amended 1994 Ky. Acts ch. 460, sec. 8, effective July 15, 1994. -- Amended 1990 Ky. Acts ch. 432, sec. 1, effective July 13, 1990; and ch. 496, sec. 57, effective July 13, 1990. -- Amended 1988 Ky. Acts ch. 159, sec. 1, effective July 15, 1988. -- Amended 1986 Ky. Acts ch. 237, sec. 8, effective July 15, 1986; and ch. 298, sec. 1, effective July 15, 1986. -- Amended 1984 Ky. Acts ch. 363, sec. 1, effective July 13, 1984. -- Created 1980 Ky. Acts ch. 263, sec. 1, effective July 15, 1980.

Formerly codified as KRS 224.876.

Legislative Research Commission Note. See definition of "special wastes" in KRS 224.50-760(1).

2002-2004 Budget Reference. See State/Executive Branch Budget, 2003 Ky. Acts ch. 156, pt. IX, item 41(a), at 1878; and State/Executive Branch Budget Memorandum, 2003 Ky. Acts ch. 143, at 1046 (Final Budget Memorandum, at 669).

Legislative Research Commission Note (6/20/2005). 2005 Ky. Acts chs. 11, 85, 95, 97, 98, 99, 123, and 181 instruct the Reviser of Statutes to correct statutory references to agencies and officers whose names have been changed in 2005 legislation confirming the reorganization of the executive branch. Such a correction has been made in this section.