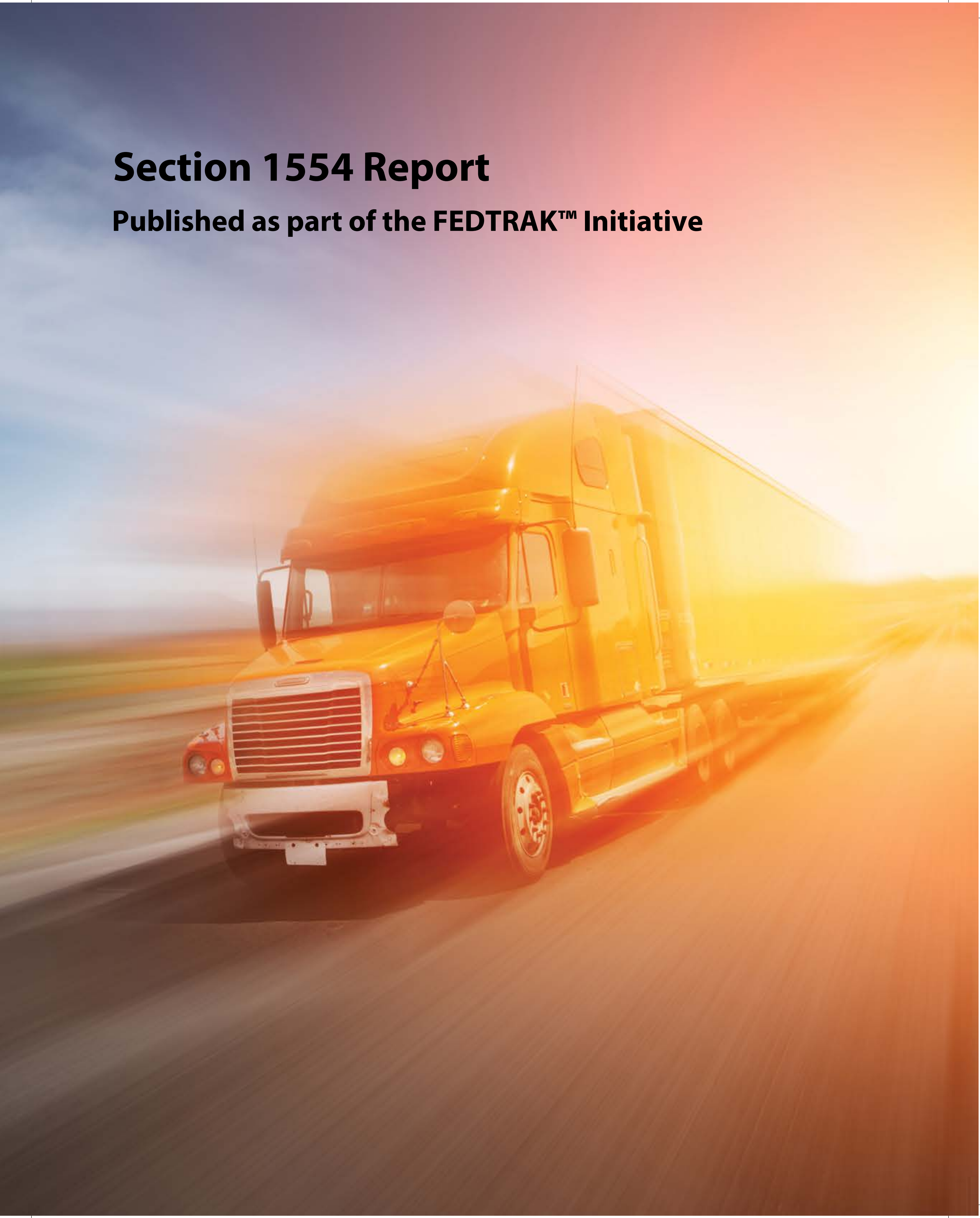
Section 1554 Report

Published as part of the FEDTRAK™ Initiative



INTRODUCTION

On August 3, 2007, President Bush signed the "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act). Section 1554 of the 9/11 Act directs the United States Transportation Security Administration (TSA) to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials. In developing its tracking program, Congress directed TSA to take into consideration the findings and recommendations of the Federal Motor Carrier Safety Administration's (FMCSA) **Hazardous Materials Safety & Security Operational Field Test**, completed in 2004, and TSA's **Hazmat Truck Security Pilot**, completed in 2007.

FMCSA's Hazardous Materials Safety & Security Operational Field Test was a seminal study examining the use of truck telematics technology to enhance hazmat shipment safety and security. It was the first and only large-scale test of truck telematics technology, and is particularly notable because the FMCSA project team quantified the costs and benefits associated with telematics technology deployment by hazmat carriers.

TSA's Hazmat Truck Security Pilot, a Congressionally-mandated initiative, was designed to determine if a centralized data processing/tracking center for hazmat shipments, was technically feasible. It is notable because the Pilot proved that a centralized shipment tracking center is, in fact, feasible.

Congress also directed TSA to evaluate eight cost and technology items listed in Section 1554(a)(2)(c) as it develops its shipment tracking program. Essentially, evaluation of these cost and technology items will update the findings and recommendations of FMCSA's Hazardous Materials Safety & Security Operational Field Test and TSA's Hazmat Truck Security Pilot in the context of the regulatory, market, and programmatic conditions that exist today. For example, Section 1554 (a)(2)(c)(i) requires TSA to evaluate any new information related to the costs and benefits of deploying, equipping and utilizing tracking technology. This update is important to the development of TSA's shipment tracking program because the Hazardous Materials Safety & Security Operational Field Test was completed in 2004 and the Hazmat Truck Security Pilot in 2007. However, the market, regulatory, and programmatic context for hazmat transportation, especially for the riskiest hazmat shipments, has changed significantly since these studies were completed.

The Kentucky Transportation Center of the University of Kentucky was tasked with completing an independent analysis of the cost and technology evaluations listed in Section 1554(a)(2)(c) with the objective of helping TSA decide how to move forward in meeting its shipment tracking mandate under Section 1554. In developing its recommendations, the project team took special note of the language of Section 1554 that calls on TSA to collaborate with DOT as TSA develops its shipment tracking program. This language reflects the legislative and programmatic roles of TSA and DOT in the management of the Federal hazmat program, with TSA responsible for hazmat transportation security and with DOT responsible for hazmat transportation safety.

The project team conducted a detailed literature review of the telematics product/service offerings, both in the United States and in other countries, and followed up with visits to prominent telematics service providers in the United States and Canada. The project team also met with representatives of Singapore's Civil Defense Force (SCDF), Singapore's homeland security agency, to evaluate Singapore's Hazmat Transport Vehicle Truck Security System, a hazmat tracking system that the SCDF implemented to prevent terrorists from using hazmat shipments as weapons.

The focus of the visits to the U.S.- and Canadian-based telematics service providers was to probe deeply into the products and services they offer as well as their interest in refining their product/service offerings to meet TSA's highway hazmat security needs. Data on technology functionality and telematics system unit costs (capital and operating) was collected by the project team during the visits. While cost and technology data was critical to downstream benefit/cost analyses, information collected during the visits provided the project team with a rich body of qualitative information that also helped the team address a number of pressing programmatic questions facing TSA, including the following:

What telematics functionality should be included in tractor- and trailer-based telematics system to meet the security challenges facing TSA's highway program?[1]

How well do the product/service offerings from U.S.-based telematics service providers serve TSA's highway hazmat security needs? Are there gaps? If so, are U.S. telematics service providers willing to invest to refine their product/service offerings to meet TSA needs?

Do the telematics systems offered in other countries incorporate security functionality not offered widely in the United States, especially telematics functionality related to shipment hijacking?

What are the security benefits of wide-scale deployment of truck telematics systems by Tier 1 Highway Security Sensitive Materials (HSSM) carriers? What will it cost HSSM carriers to deploy telematics systems that satisfy TSA's security needs?

Is a regulatory program that requires technology deployment and data reporting to a centralized shipment tracking center justified on a benefit/cost basis?

How should TSA move forward in developing a shipment tracking program that meets the spirit and intent of Section 1554? What concept of operation plan would drive such a program?

Section I of this report explores the historical development of the Federal hazmat program, both at DOT and TSA, and places the 9/11 Act and Section 1554 in historical and programmatic context. **Section II** examines basic truck telematics technology and the market trends underlying the telematics market in the United States and in other countries. **Section III** contains the project team's technology recommendations for Tier 1 HSSM telematics systems. **Section IV** presents the project team's thoughts on an overall concept of operation plan for TSA's highway hazmat security program and **Section V** examines benefits and costs associated with that highway hazmat security program. **Section VI** presents the project team's Section 1554 summary recommendations related to the requirements of Section 1554 of the 9/11 Act.

The recommendations in Section VI represent the views of the Kentucky Transportation Center of the University of Kentucky, and are presented as independent recommendations for TSA to consider as it crafts its strategy for implementing the requirements of Section 1554 of the 9/11 Act.

In Section VI, the project team recommends that TSA move forward on a regulatory program that will require Tier 1 HSSM carriers to deploy tractor- and trailer-based telematics systems and report data to a Public Sector Reporting Center (PSRC) as part of a Tier 1 HSSM shipment tracking program under Section 1554 of the 9/11 Act. The security benefits of a Tier 1 HSSM tracking program, quantified in FMCSA's landmark *Hazardous Materials Safety & Security Operational Field Test*, far outweigh the cost of that program.

The project team recommends that TSA require Tier 1 HSSM carriers to deploy telematics systems that meet specific security challenges in the hazmat supply chain, especially the threat of hijacking, and that TSA's telematics initiative build on the technology/data platform underlying DOT's Electronic On Board Recorder. Also, the team recommends that TSA implement an electronic manifest system (chain-of-custody) for Tier 1 HSSM shipments and embed risk management capabilities into systems underlying the Public Sector Reporting Center. As an immediate priority, the project team recommends that TSA complete development of an "emergency-ready" Tier 1 HSSM shipment tracking/chain-of-custody system as quickly as possible. Lastly, the project team recommends that TSA establish September 11, 2016, the 15th anniversary of the attacks on the World Trade Towers and the Pentagon, as the "go-live" date for TSA's Section 1554 shipment tracking program.

• • •

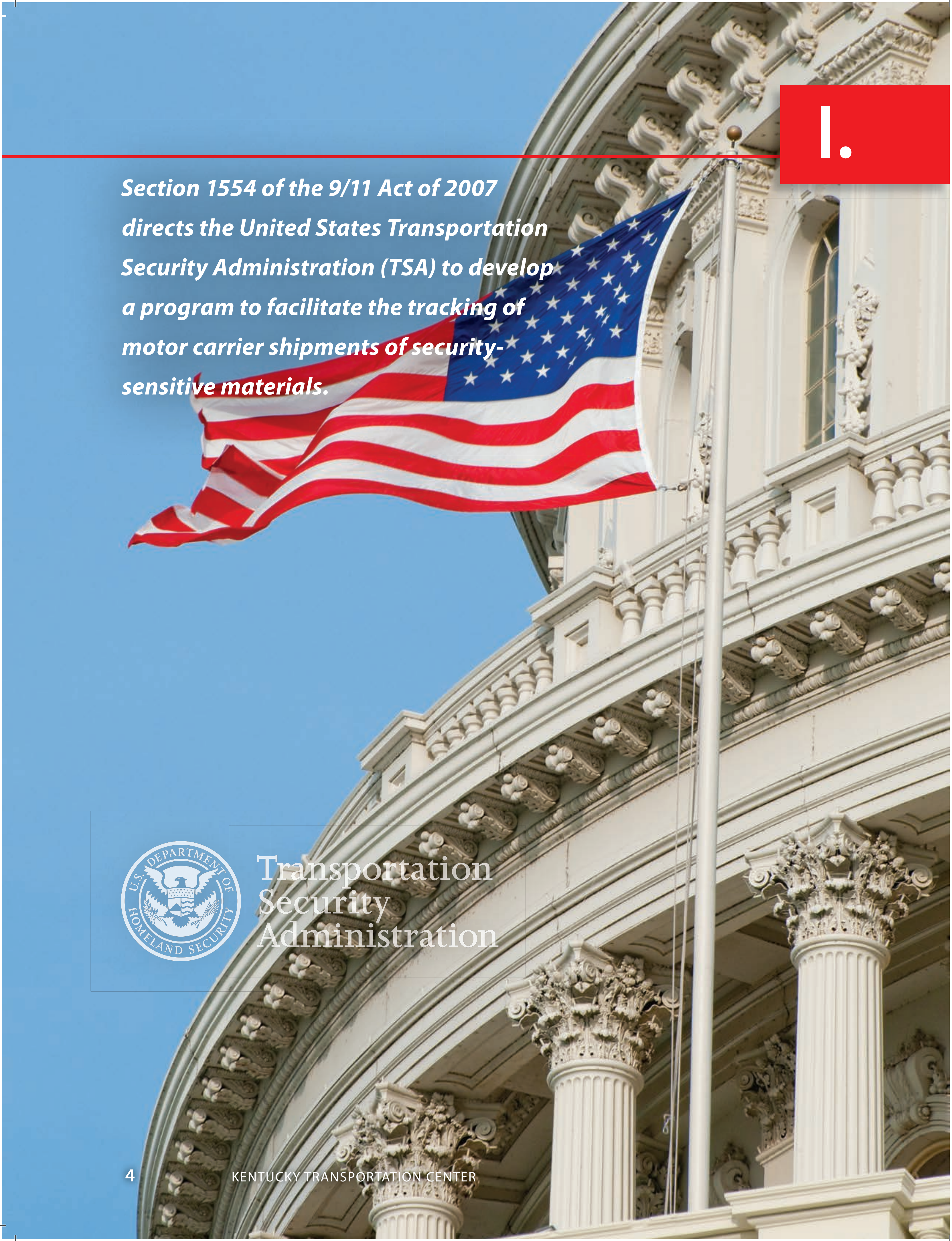
[1] TSA defines Tier 1 Highway Security Sensitive Materials (HSSMs) as "HSSM transported by motor vehicle whose potential consequences from an act of terrorism include a highly significant level of adverse effects on human life, environmental damage, transportation system disruption, or economic disruption."

TABLE OF CONTENTS

Sidebars

I.

Section 1554 of the 9/11 Act of 2007 directs the United States Transportation Security Administration (TSA) to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials.



Transportation
Security
Administration

FEDERAL HAZMAT SECURITY TIMELINE

On August 3, 2007, President Bush signed the "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act). Section 1554 of the 9/11 Act directs the United States Transportation Security Administration (TSA) to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials.

As illustrated in the timeline in **Figure I-1**, a tremendous amount of activity at the Federal level preceded the 9/11 Act legislation.

On November 19, 2001, the United States Transportation Security Administration (TSA) was created and placed in the United States Department of Transportation (DOT) with the passage of the Aviation and Transportation Security Act. The Act gave DOT broad responsibility and authority for ``security in all modes of transportation'' (49 U.S.C. 114(d)). In the highway mode, the Act gave DOT the Federal responsibility for regulating the safety and security of highway shipments of hazardous materials.

On July 16, 2002, DOT issued an Advanced Notice of Proposed Rulemaking (ANPRN) that asked for comment on the need for enhanced security requirements for the motor carrier transportation of hazardous materials. DOT sought comments on the feasibility of specific security enhancements and the potential costs and benefits of deploying such enhancements. The ANPRN is notable in that it highlighted Federal concern about terrorist plans to use hazmat shipments as weapons and signaled DOT's clear intent to enhance security in the hazmat supply chain via a regulatory mechanism. It is also exceptionally notable in that the ANPRN was published eleven years ago. As noted in **Sidebar 1**, security measures discussed in the ANPRN include vehicle tracking and anti-theft devices.

DOT followed the ANPRN with a March 25, 2003 rule requiring high risk hazmat shippers and carriers to prepare and follow a written security plan including security measures for en-route shipments. And on June 30, 2004, DOT issued a rule requiring high risk hazmat carriers to obtain a hazmat safety permit that includes measures for driver/carrier communications.

Security Requirements for Motor Carriers Transporting Hazardous Materials Advanced Notice of Proposed Rulemaking (Federal Register July 16, 2002)

Background

Over 800,000 shipments of hazardous materials occur each day in the United States. The overwhelming majority of these shipments—approximately 95 percent—are made by highway. Many of the hazardous materials transported by motor carriers potentially may be used as weapons of mass destruction or in the manufacture of such weapons. Since September 11, 2001, on several occasions, Federal law enforcement officials provided information indicating that terrorist organizations may be planning to use motor vehicles transporting certain hazardous materials for additional terrorist attacks on facilities in the United States.

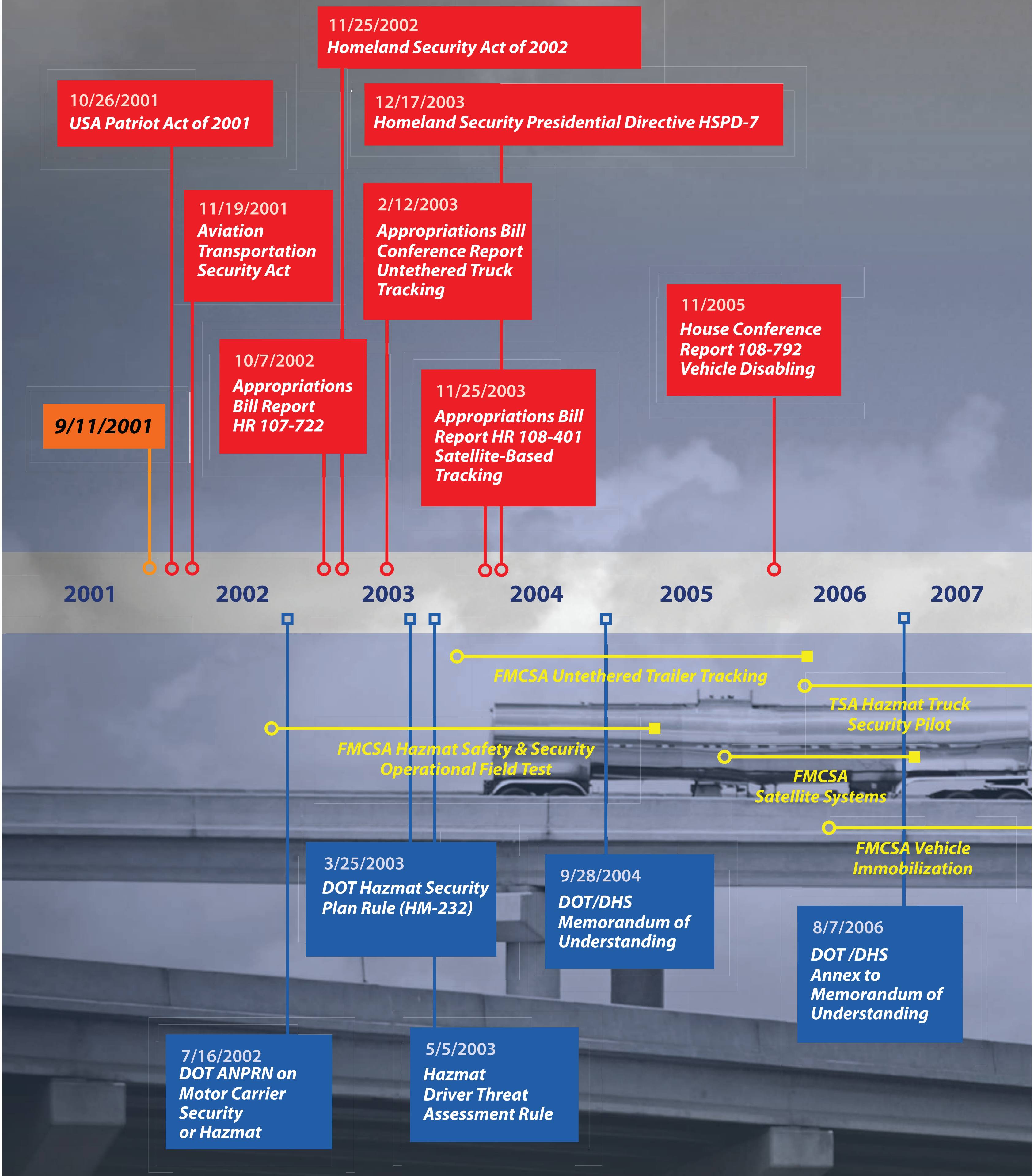
Purpose of this ANPRN

RSPA and FMCSA are seeking information on the feasibility of imposing specific security requirements on motor carriers that transport hazardous materials in commerce. Certain government agencies, including the Department of Defense (DoD), the Department of Energy (DOE), and the Nuclear Regulatory Commission, as well as some private companies, employ rigorous security measures to protect sensitive shipments. Some of these security measures may also be appropriate for broader application to commercial motor carrier shipments of hazardous materials. In addition, there are many technological solutions for tracking shipments, communicating with drivers, or securing shipments within trailers that can protect shipments from hijacking or provide an early indication of a potential security problem.

Vehicle Tracking. Satellite tracking, direct short-range communications, and cell phone technologies enable motor carriers to monitor a shipment while en route to its destination and to identify and communicate deviations from prescribed routes or time frames. Relatively sophisticated systems are currently available and are already used by many motor carriers to deter theft. Increasing numbers of motor carriers utilize vehicle tracking systems to enhance shipment security.

Anti-Theft Devices. There are a number of anti-theft devices that can help to reduce the risk of vehicle hijacking or cargo theft. Devices such as remote vehicle shut-offs, electronic ignition locks, and driver verification systems utilizing security codes or fingerprints assure that unauthorized persons cannot operate a motor vehicle. Tamper-resistant or tamper-evident seals and locks on cargo compartment openings protect sensitive shipments.

SIDEBAR 1.



9/11/2001

10/26/2001 USA Patriot Act of 2001

11/19/2001 Aviation Transportation Security Act

10/7/2002 Appropriations Bill Report HR 107-722

11/25/2002 Homeland Security Act of 2002

2/12/2003 Appropriations Bill Conference Report Untethered Truck Tracking

11/25/2003 Appropriations Bill Report HR 108-401 Satellite-Based Tracking

12/17/2003 Homeland Security Presidential Directive HSPD-7

11/2005 House Conference Report 108-792 Vehicle Disabling

7/16/2002 DOT ANPRN on Motor Carrier Security or Hazmat

3/25/2003 DOT Hazmat Security Plan Rule (HM-232)

5/5/2003 Hazmat Driver Threat Assessment Rule

9/28/2004 DOT/DHS Memorandum of Understanding

8/7/2006 DOT /DHS Annex to Memorandum of Understanding

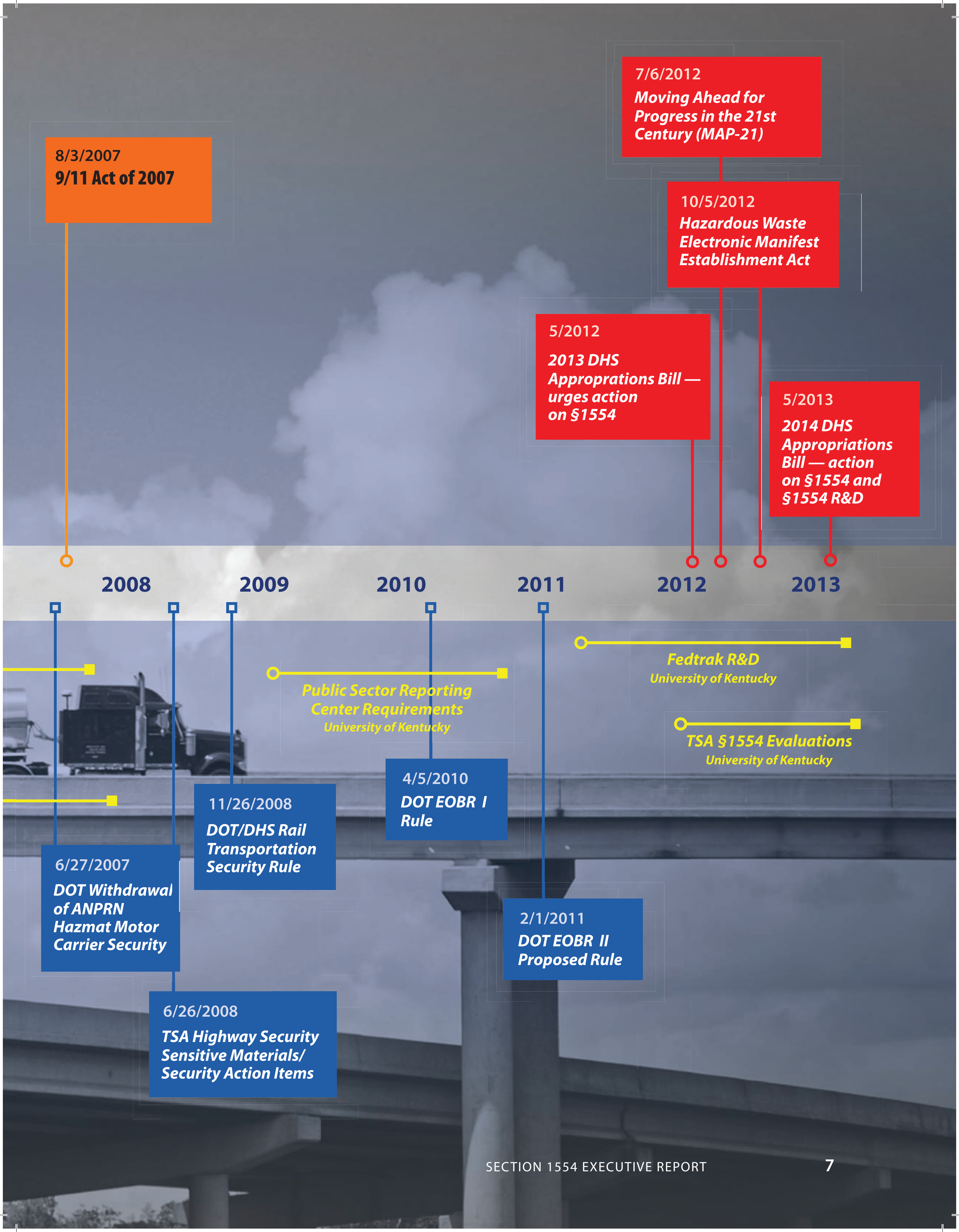
FMCSA Untethered Trailer Tracking

TSA Hazmat Truck Security Pilot

FMCSA Hazmat Safety & Security Operational Field Test

FMCSA Satellite Systems

FMCSA Vehicle Immobilization



8/3/2007
9/11 Act of 2007

7/6/2012
Moving Ahead for Progress in the 21st Century (MAP-21)

10/5/2012
Hazardous Waste Electronic Manifest Establishment Act

5/2012
2013 DHS Appropriations Bill — urges action on §1554

5/2013
2014 DHS Appropriations Bill — action on §1554 and §1554 R&D

Fedtrak R&D
University of Kentucky

Public Sector Reporting Center Requirements
University of Kentucky

TSA §1554 Evaluations
University of Kentucky

4/5/2010
DOT EOBR I Rule

11/26/2008
DOT/DHS Rail Transportation Security Rule

6/27/2007
DOT Withdrawal of ANPRN Hazmat Motor Carrier Security

2/1/2011
DOT EOBR II Proposed Rule

6/26/2008
TSA Highway Security Sensitive Materials/ Security Action Items

DOT, and later TSA, also completed a series of Congressionally-mandated studies intended to lay the foundation for a hazmat security regulatory program based on the deployment of truck telematics systems and data reporting to a shipment tracking center. The studies include the following.

- FMCSA Hazardous Materials Safety and Security Technology Field Operational Test (2002-2004)
- FMCSA Untethered Trailer Tracking Report (2004-2005)
- FMCSA Vehicle Immobilization Technologies (2005-2007)
- FMCSA Expanded Satellite-Based Tracking System Requirements (2005-2006)
- TSA Hazmat Truck Security Pilot (2005-2007)

In addition, TSA is currently funding the Fedtrak R&D initiative, a project begun initially by Department of Homeland Security's Science & Technology Directorate in 2009 to extend the work completed in TSA's Hazmat Truck Security Pilot. The Fedtrak R&D initiative is focused on building software to support an operational shipment tracking/risk management center for high risk hazardous materials.

On November 25, 2002, the United States Department of Homeland Security (DHS) was created by the Homeland Security Act of 2002. Along with a number of other agencies, the Act moved TSA into DHS. With this move, completed March 2003, Congress split responsibility for the Federal hazmat mission - with DOT retaining responsibility for hazmat safety and DHS/TSA with responsibility for hazmat security.

On December 17, 2003, Homeland Security Presidential Directive Number 7 (HSPD-7) reaffirmed TSA's authority over security in all transportation modes and directed DOT and DHS to "collaborate in regulating the transportation of hazardous materials in all modes." On September 28, 2004, DOT and DHS signed a Memorandum of Understanding (MOU) on Roles and Responsibilities. The purpose of the MOU was to facilitate the development and deployment of transportation security measures that promote safety, security, and efficiency in the movement of people and goods. An Annex to the MOU was issued on August 7, 2006 that was even more specific about relative roles and responsibilities.

Establishment of the MOU between DOT and DHS/TSA, including the Annex to the MOU, was a watershed event in the history of the Federal hazmat security program. It formalized the relationship between DHS and DOT on hazmat regulation and oversight, and formalized the relative roles and responsibilities of each agency. To DOT and TSA hazmat stakeholders, it signaled the transition of hazmat security responsibilities from DOT to TSA. On June 27, 2007, DOT withdrew its 2002 ANPRN.

The MOU is also important because it established an expectation of substantive collaboration between TSA and DOT in their joint management of the Federal hazmat program. This collaboration is a critical success factor for the Federal hazmat program as it is impossible to fully separate the hazmat safety and security missions. In fact, as illustrated in **Figure I-2**, they are dependent and mutually reinforcing.

The Venn diagram in Figure I-2 illustrates the overlap of the safety and security missions for high risk hazmat shipments. Note that the DOT/TSA Memorandum of Understanding has the effect of "pushing" DOT toward TSA's security mission while the 9/11 Act legislation has the effect of "pushing" TSA toward DOT's safety mission. The net effect is an overlap of the missions of the two agencies and a greatly enhanced opportunity for collaboration. As Figure I-2 illustrates, this overlap is substantial and encompasses a number of high priority items for both DOT's safety mission and TSA's security mission.

Underlying the MOU was the hope that a mutually beneficial "virtuous circle" would be forged between TSA and DOT as each managed its share of the Federal hazmat program.[1] In the context of a virtuous circle, strengthening safety measures for high risk hazmat shipments would tend to reinforce the security of those shipments. Conversely, strengthening security measures would tend to reinforce shipment safety. For example, a DOT initiative to use electronic shipping papers to improve first responder hazard communications could also provide

[1] The term, virtuous circle, is a set of events or situations that work together in synergy to generate favorable outcomes for multiple parties. A feedback loop helps to perpetuate a virtuous circle and the positive outcomes it generates. A virtuous circle is the opposite of a vicious cycle which generates detrimental outcomes for the parties.

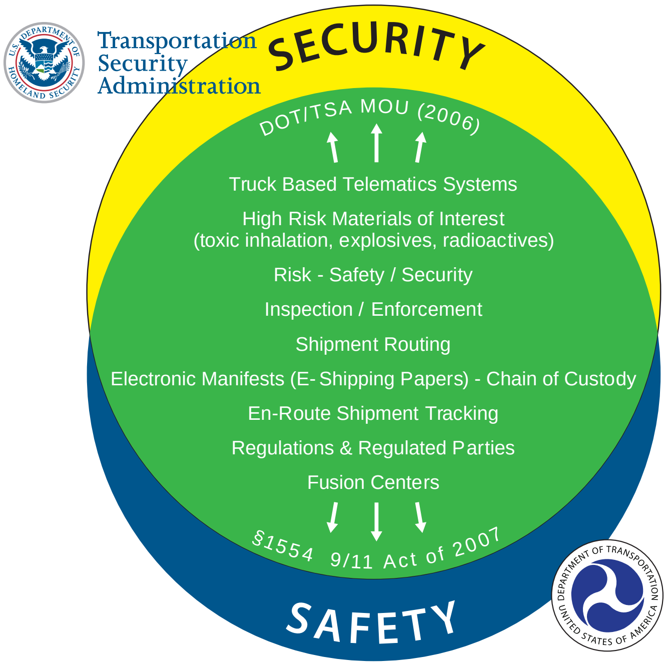

Transportation Security Administration
SECURITY
DOT/TSA MOU (2006)
Truck Based Telematics Systems
High Risk Materials of Interest
(toxic inhalation, explosives, radioactives)
Risk - Safety / Security
Inspection / Enforcement
Shipment Routing
Electronic Manifests (E- Shipping Papers) - Chain of Custody
En-Route Shipment Tracking
Regulations & Regulated Parties
Fusion Centers
§1554 9/11 Act of 2007
SAFETY

Figure I-2. Federal hazmat mission overlap

chain-of-custody control for shipments of high risk hazardous materials, a significant boost to TSA's highway hazmat security program.[2]

On August 3, 2007, President Bush signed the "Implementing Recommendations of the 9/11 Commission Act of 2007" (the 9/11 Act). Section 1554 of the 9/11 Act directs TSA to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials in consultation with DOT. Section 1554 requires TSA to develop its truck tracking program to reflect the results of two initiatives completed prior to the 9/11 Act: 1). FMCSA's Hazardous Materials Safety & Security Operational Field Test; and 2). TSA's Hazmat Truck Security Pilot program.

FMCSA's Hazardous Materials Safety & Security Operational Field Test was the first and only large-scale test of truck telematics technology. The objective of the study was to determine the extent to which existing security vulnerabilities in the hazmat supply chain might be reduced by the deployment of truck telematics technology such as GPS tracking, wireless modems, panic buttons, and on-board computers. The Hazardous Materials Safety & Security Operational Field Test 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. The Hazardous Materials Safety & Security Operational Field Test concluded that truck telematics will generate significant security benefits via the reduction of supply chain risk as well as significant operational benefits for hazmat carriers.

After the FMCSA finished the Hazmat Safety and Security Technology Field Operational Test in November 2004, Congress directed TSA to undertake the TSA Hazmat Truck Security Pilot project. The purpose of the pilot was to determine if 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. A technology prototype of a basic shipment tracking system was built and tested, including the development and testing of communication protocols to allow alerts and tracking information to be transmitted from commercially available tracking systems to the prototype truck tracking system. Although the technology prototype system fell far short of an operational tracking system, the Hazmat Truck Security Pilot program demonstrated that a truck tracking system is feasible from a technology and systems perspective.

Beyond FMCSA's Hazmat Safety and Security Technology Field Operational Test and TSA's Hazmat Truck Security Pilot, Section 1554(a)(2)(c) of the 9/11 Act also specifically listed eight items that TSA must take into consideration as it develops its truck tracking program. They are presented in **Sidebar 2**. In essence, the eight evaluation items direct TSA to assess the findings from FMCSA's Hazardous Materials Safety & Security Operational Field Test and TSA's Hazmat Truck Security Pilot in relation to market, regulatory, and programmatic conditions that exist today. This is important because FMCSA's Hazardous Materials Safety & Security Operational Field Test was completed in 2004 and the Hazmat Truck Security Pilot in 2007, and the market, regulatory, and programmatic context for hazmat transportation, especially for the riskiest hazmat

[2] Refer to Section 33005, Moving Ahead for Progress in the 21st Century Act (MAP-21) authorizing electronic shipping paper pilot studies.

shipments, has changed significantly since these studies were completed.

On June 26, 2008, TSA issued Security Action Items (SAIs) for Highway Security Sensitive Materials (HSSMs). TSA defines Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSMs) as "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." Tier 1 HSSMs include toxic inhalation gases, explosives and radioactive materials.

There are about 2 million Tier 1 HSSM shipments per year in the United States – well less than 1 percent of all hazmat shipments. TSA's decision to focus on the riskiest hazmat shipments was a hugely important step in the evolution of TSA's highway hazmat security program. Focusing attention on about 2 million hazmat shipments is eminently manageable from a shipment tracking perspective. And by focusing on this subset of risky materials, TSA brought its highway hazmat security program into alignment with DOT's hazmat safety permitting program and upcoming DOT/TSA rail security regulations, both of which regulate essentially the same subset of highly risky hazardous materials.

TSA, along with DOT, issued rail security regulations in October 2008 that focused on risk reduction and shipment routing for high risk hazmat shipments. The United States Customs and Border Protection (CBP) completed the phase-in of its truck e-manifest program in 2008 requiring carriers to submit an electronic manifest for shipments of all goods entering the United States by truck from Canada and Mexico. The United States Environmental Protection Agency sought and received authority under Hazardous Waste Electronic Manifest Establishment Act (PL 112-195) in 2012 to move toward the implementation of an electronic manifest program for shipments of hazardous waste, a subset of the larger hazmat universe.

More recently DOT's hazmat safety program has moved forward in advancing the deployment of truck telematics with DOT's EOBR/Hours of Service initiative. DOT issued its EOBR I rule in April 2010 and its proposed EOBR II rule in February 2011. A final EOBR rule is expected in 2013, with full deployment of EOBRs by commercial vehicles in 2015.

Section 1554 (a) of the 9/11 Act

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

(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.

SIDEBAR 2.

Congressional interest in TSA's highway hazmat security program and implementation of Section 1554 remains strong. House Report 113-091 accompanying the FY2013 DHS Appropriations Bill encouraged TSA to move forward on implementing the requirements of Section 1554 of the 9/11 Act.[3] House Report 113-091 accompanying the 2014 DHS Appropriations Bill included language that more insistently urged TSA to move forward on developing its shipment tracking program under Section 1554 including R&D activities.

TIMELINE TREND CONCLUSIONS

The hazmat timeline in **Figure I-1** makes it easier to view developments in the Federal hazmat program over time. The project team's summary of macro-level trends and events along the timeline follows.

1. In the early 2000's, as evidenced by DOT's highway security 2002 ANPRN, DOT and Congress believed there was a significant security threat in the hazmat supply chain and that a regulatory program that required hazmat carriers to install telematics systems and report data to a centralized tracking facility was needed.

2. DOT, at the behest of Congress, initiated and completed a number of large scale studies to lay the foundation for a hazmat security regulatory program including FMCSA's Hazmat Safety and Security Technology Field Operational Test. TSA also later added to the body of research needed to support a highway hazmat security program by completing its Hazmat Truck Security Pilot.

3. TSA moved from DOT to DHS when DHS was created. The transition of the hazmat security program to TSA took several years, and the DOT/DHS Memorandum of Understanding was an important milestone that reflected the transition of responsibility for the Federal hazmat security mandate by DHS/TSA.

4. DOT laid down a strong foundation for the Federal highway hazmat security program, and the 9/11 Act of 2007 was a clear statement by Congress that it wanted TSA to move forward on implementing its highway hazmat security program including shipment tracking and the deployment of telematics systems by carriers hauling high risk materials.

   Issuance of Security Action Items in 2008 was a positive first step by TSA toward development of a highway hazmat security program that would satisfy the requirements of Section 1554 of the 9/11 Act. TSA's Security Action Items have no regulatory force, however, and compliance is voluntary on the part of HSSM shippers, carriers and consignees. But in issuing its Security Action Items, TSA essentially laid down a placeholder for future regulations, especially those that might flow out of a tracking program developed under Section 1554 of the 9/11 Act.

5. DOT has moved steadily forward with the highway safety program including its EOBR/Hours of Safety initiative which draws on deployment of basic telematics systems by operators of commercial vehicles. The absence of a "virtuous circle" between DOT's hazmat safety and TSA's hazmat security program has resulted in a disjointed approach to the Federal hazmat mission and missed opportunities for collaboration and cross-program efficiencies.

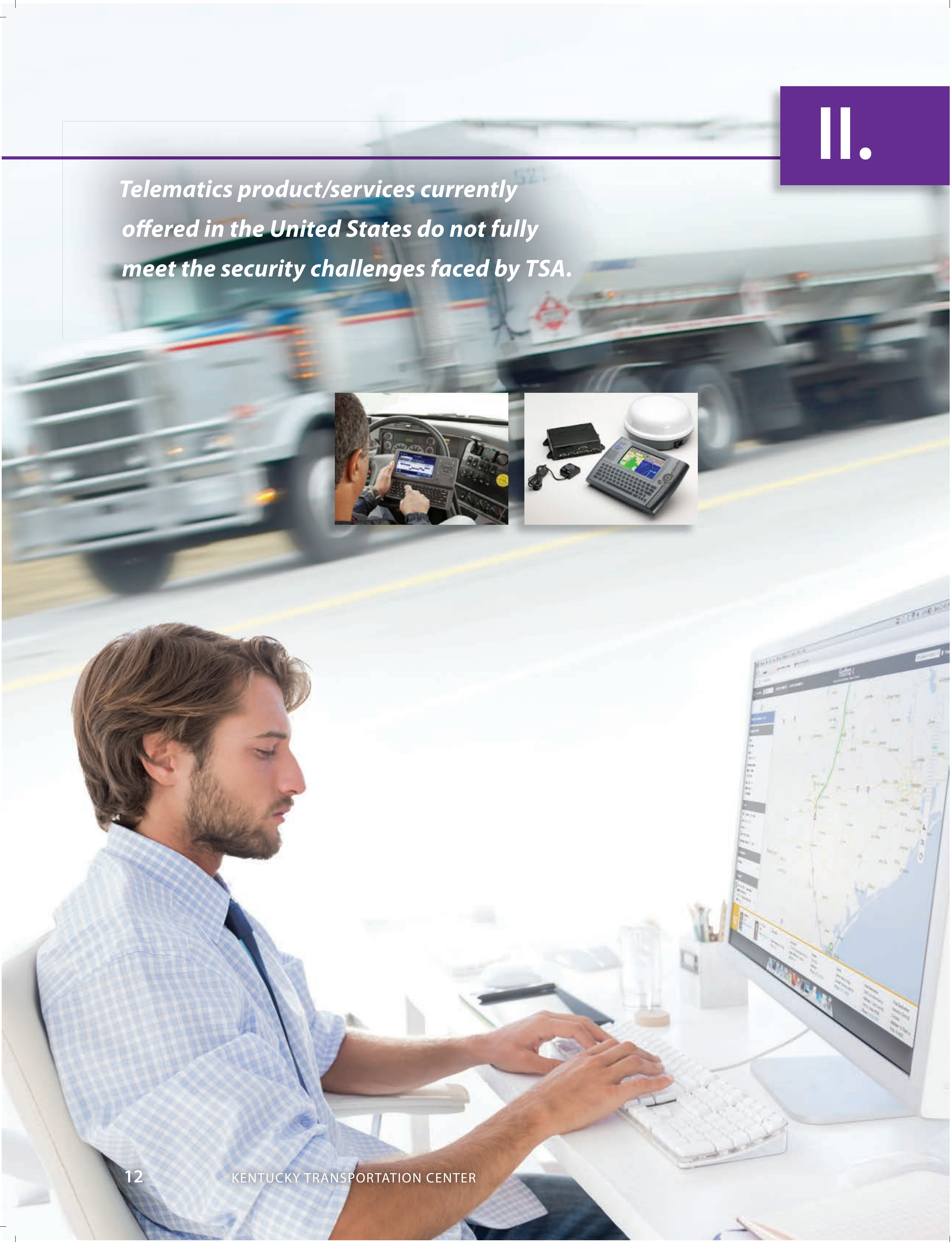
6. Language in House reports accompanying FY2013 and FY2014 DHS Appropriation bills makes it clear that Congress is resolute in its expectation that TSA develop a shipment tracking program as directed by Section 1554 of the 9/11 Act.

• • •

[3] Refer to Report 113-91; Department of Homeland Security Appropriations Bill, 2014; page 59.

II.

Telematics product/services currently offered in the United States do not fully meet the security challenges faced by TSA.



As illustrated in **Figure II-1** (pgs.14-15), a typical trucking telematics system connects tractor- and trailer-mounted telematics devices to a commercial fleet tracking data center via a wireless modem. This set-up allows fleet managers to track the location and status of the tractors and trailers in their fleets on a real-time basis via an internet connection. Fleet managers also use GIS tools (mapping, routing, reporting) and in-cab messaging systems to monitor and manage fleet activity.

TSA's telematics focus is on Tier 1 Highway Security Sensitive Materials carriers and the security threats associated with Tier 1 HSSM shipments.

TSA issued Security Action Items (SAIs) for Highway Security Sensitive Materials (HSSMs) on June 26, 2008. TSA defines Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSMs) as *"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."* TSA-designated Tier 2 HSSMs also pose a risk from a security perspective, but to a lesser extent. As illustrated in **Figure II-2**, Tier 1 HSSMs include explosives, toxic inhalation gases, and radioactive materials. There are about 2 million Tier 1 HSSM shipments in the United States each year, far less than 1% of all hazmat shipments.

TSA TIER 1 HIGHWAY SECURITY SENSITIVE MATERIALS
 Division 1.1, Division 1.2, Division 1.3 Explosives
 Division 2.3 Toxic (Poison) Gas
 Class 7 Radioactive Materials
FLAMMABLE 3 NON-FLAMMABLE GAS 2 POISON 6 CORROSIVE 8 Class 3 Flammable Liquids Division 2.2 Non-Flammable Gas Division 6.1 Poisonous Materials Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation)
Other Materials Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules.

Figure II-2.

At the same time it released its HSSM lists, TSA released Security Action Items (SAIs) for HSSM shipments. The SAIs are voluntary, "good business practices" that TSA recommends shippers, carriers, and consignees of HSSM shipments implement. As illustrated in **Figure II-3**, SAIs 1-23 apply to all HSSM En-Route shipments and SAIs 17-23 apply specifically to en-route Tier 1 HSSM shipments.

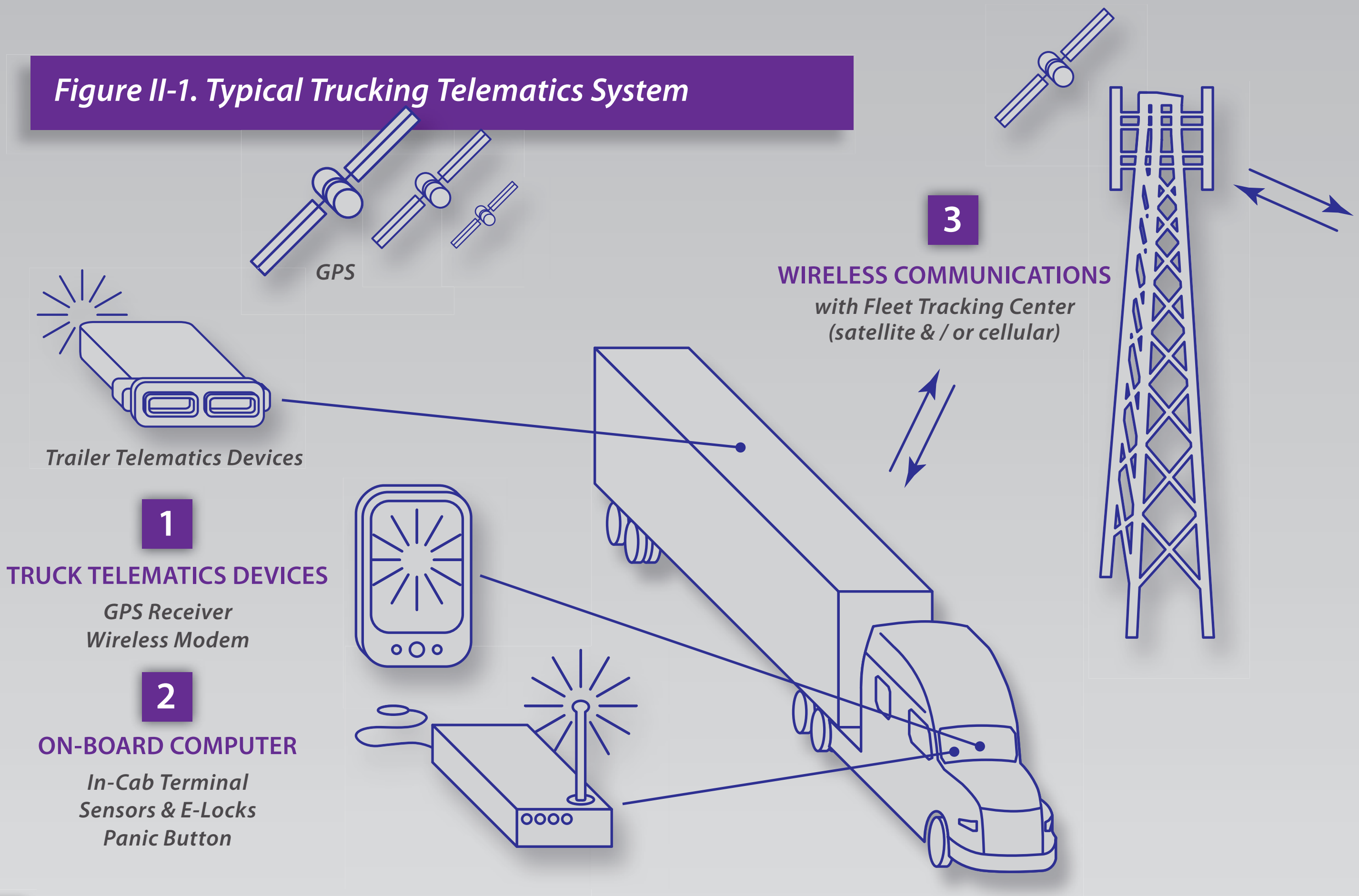
TSA has focused its highway hazmat security program on Tier 1 HSSM shipments, and threats associated with these shipments as illustrated in **Figure II-4**. TSA's SAIs were developed by TSA with the expectation that Tier 1 HSSM carriers would deploy telematics to reduce the likelihood that Tier 1 HSSM shipments can be used by terrorists as weapons. Three SAIs touch specifically on the use of telematics for vehicles hauling 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

Figure II-1. Typical Trucking Telematics System



1 **TRACTOR/TRAILER TELEMATIC DEVICES** — At the heart of every tractor telematics system are two components – a GPS receiver and a wireless modem. The GPS receiver is used to pinpoint the exact physical location of the truck using signals received from GPS satellites. The location of the truck is transmitted to a fleet tracking center via the truck's wireless modem over a wireless communications network. Additional devices add telematics functionality. For example, sensors and telemetric devices can monitor a wide variety of truck conditions such as brake wear, tire pressure, engine RPM, 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 often connected to an on-board computer include electronic locks, panic buttons, and biometric devices. Telematics devices connected to an on-board computer can be monitored and/or activated remotely as long as there is a wireless connection to the truck's on-board computer. An in-cab terminal allows a driver to interact with the truck telematics system and to communicate with the fleet manager or back-end fleet operations center. Trailer telematics systems are usually installed as separate, stand-alone telematics systems, but are similar in function to tractor telematics systems. A GPS receiver and wireless modem connect the trailer to a backend data center and the fleet manager. Unlike tractor-based telematics systems which are powered by the tractor's electrical system, trailer telematics systems are usually powered by batteries.

2 **ON-BOARD COMPUTER (OBC)** — An on-board computer, often called a "black box", 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 on-board computer is connected to the truck's J-bus so it can monitor all the truck's electronic systems and to the truck's wireless modem enabling a wireless internet connection on the truck. Various truck telematics devices and sensors can be connected to the on-board computer and monitored and controlled by the fleet operations center via the wireless connection. Devices/services that the on-board computer/wireless setup enables include the following.

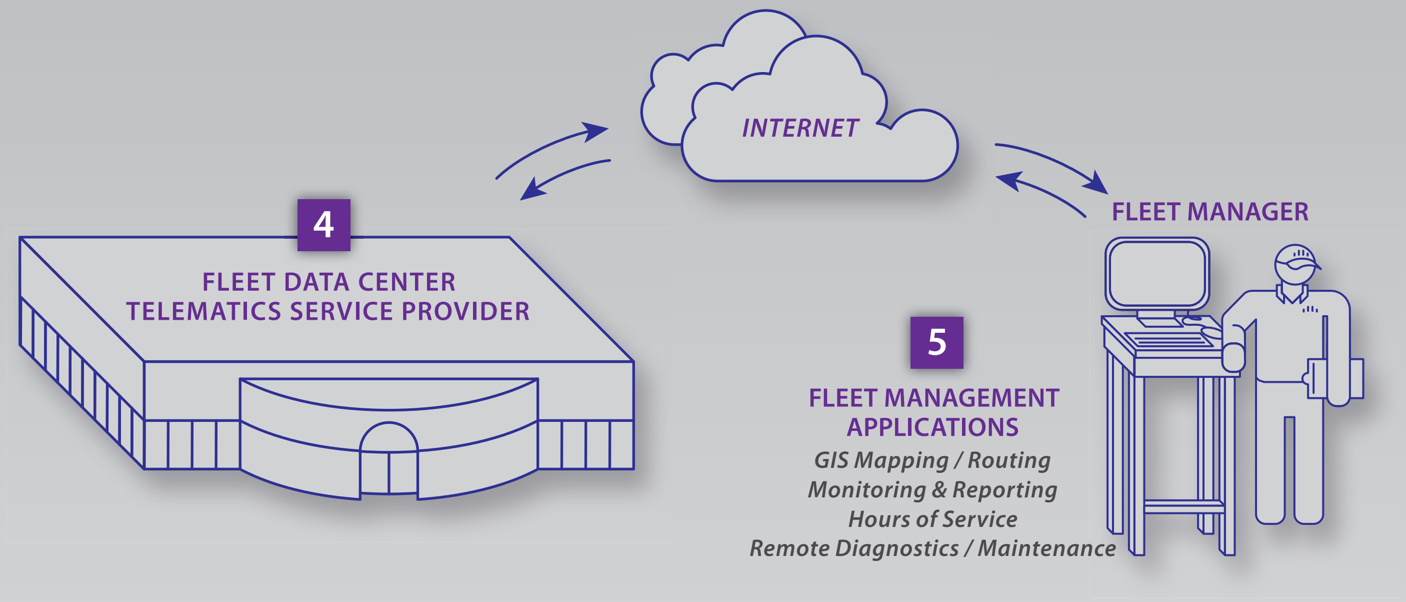
Driver access to web services and back-office systems. The on-board computer/wireless modem setup essentially allows the truck to become a rolling office. The driver can use a data terminal or a mobile device and the truck's wireless internet connection to tie to web services and corporate back-office 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 operations center &/or fleet dispatchers. If paired with an on-board computer, a driver-carried panic button can be used to remotely disable the truck.

E-locks and vehicle disabling. Connecting the on-board computer/wireless modem with vehicle operating systems allows dispatcher-initiated remote vehicle shutdowns and trailer door locking/unlocking. Electronic cargo locks (e-locks) detect unauthorized cargo access, especially important between shipment gate-out and gate-in.

Security alert. Connecting the on-board computer/wireless modem with vehicle operating systems allows security alerts to be sent to pre-established contacts when onboard sensors such as e-locks, tamper detection, trailer disconnect are triggered.

In-cab terminal. Connecting the on-board computer/wireless modem with the in-cab terminal allows the in-cab terminal to serve as a log-in device. An alert will be sent to fleet operations center or dispatch if an unauthorized person attempts to operate the truck. Smart cards, biometric devices, or PIN/Passwords can serve as the driver authorization mechanism.



3 **WIRELESS COMMUNICATION** — A truck telematics system interacts with a fleet operations center via wireless modem and a wireless communications network. A 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 that use GSM/GPRS cellular wireless networks have experienced tremendous growth over the past decade. GSM/GPRS cellular systems provide extensive national coverage and are less expensive than satellite communication systems. Most telematics service providers offer hybrid satellite/cellular systems that automatically switch between satellite and cellular systems based on network coverage.

4 **DATA CENTER — TELEMATICS SERVICE PROVIDER** — Telematics service providers aggregate data streaming in from the telematics systems on individual trucks and share that data with fleet managers. A challenge facing telematics service providers is the need to integrate telematics applications and functionality with enterprise data systems used by the fleet owner. Some telematics service providers have adopted an open platform approach of exposing application programming interfaces (APIs) to third-party developers, letting the third-party ecosystem take care of customization and integration.

5 **TELEMATICS SERVICE PROVIDER DATA SERVICES & FLEET APPLICATIONS** — Once a truck is connected to a telematics service provider's data center, the truck driver and the fleet manager have access to a rich selection of data services and fleet applications.

Mapping Applications — The position of a truck is transmitted over a wireless network (cellular or satellite) to a server at a fleet operations center. Software at the fleet tracking center uses truck position/location in conjunction with GIS mapping software to enable the fleet manager to view a truck's location on a map on a real-time basis. GIS tools available to the fleet manager include geo-fencing, geo-routing, geo-zoning, and mapping services.

Routing & Scheduling Applications — Software offered by telematics service providers allows fleet managers to set up efficient routes and to monitor route compliance. The software also provides fleet managers detailed operational reports. Schedule adherence provides the ability to track how well a vehicle adheres to a planned schedule and issue alerts whenever a vehicle deviates from a programmed route. Fleet managers can build schedules using their in-house routing system and upload them to a telematics service provider's data center.

Reporting Applications — Forensic software provides the fleet manager a log of location, speed, working hours, idle time, alarms and vehicle history. Activity reports provide the fleet manager access to fleet-wide location and vehicle usage data through detailed activity reports.

Driver Behavior Monitoring — Driver monitoring applications are standard for most high-end fleet management solutions. Tractor-based telematics systems log driving speeds, cornering accelerations, and heavy braking to give fleet managers the ability to track driver performance and to offer driver training based on needed areas of improvement. These applications can improve driver safety and also contribute to increased vehicle fuel efficiency and lower maintenance costs caused by poor driving practices.

Remote Diagnostics/Maintenance Applications — Maintenance is a major operating expense for commercial motor vehicles - keeping engines and other systems operating properly not only reduces repair and replacement costs, but also improves fuel efficiency, another major operational expense. Remote diagnostic applications can monitor a number of mechanical, electronic, and environmental parameters real-time and transmit data wirelessly to a telematics service provider's data center for analysis.

Hours of Service — Longstanding DOT regulations set detailed and specific requirements that limit the hours or service that a driver can remain on-duty without rest, and require drivers to maintain a log recording their hours of service. For years, drivers kept paper log books, known as the driver's "record of duty status" to track their hours of service. Electronic On Board Recorders (EOBRs) allow drivers to use an electronic log book to record hours of service information. Tractor-based telematics systems can transmit this data to a telematics service provider's data center for compilation into reports for the fleet manager.

Remote Vehicle Shutdown — The OnStar system, geared toward the consumer vehicle market, is an example of a telematics system that incorporates vehicle disabling technology. Remote vehicle shutdown capabilities are also available in telematics systems for commercial vehicles, even though they are not widely deployed.

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.

TSA HSSM 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.

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. (Tier 1 HSSM only)
18. Preplanning Routes. (Tier 1 HSSM only)
19. Security for Trips Exceeding Driver Hours of Service. (Tier 1 HSSM only)
20. Dedicated Truck. (Tier 1 HSSM only)
21. Tractor Activation Capability. (Tier 1 HSSM only)
22. Panic Button Capability. (Tier 1 HSSM only)
23. Tractor and Trailer Tracking Systems. (Tier 1 HSSM only)

Figure II-3.

The full text of TSA's Security Action Items for en-route shipments may be found in **Annex A**.

FMCSA and TSA evaluated the use of telematics to enhance safety and security in the hazmat supply chain in a series of studies dating back to 2004.

As noted in Section I, DOT issued an Advanced Notice of Proposed Rulemaking (ANPRN) in 2002 that asked for comment on the need for enhanced security requirements for the motor carrier transportation of hazardous materials. DOT sought comments on the feasibility of specific security enhancements for hazmat shipments, including the use of telematics, and the potential costs and benefits of an enhanced security program. After DOT issued the ANPR, DOT (and later TSA) completed a series of Congressionally-mandated studies intended to lay the foundation for a hazmat security regulatory program based on the deployment of truck telematics systems and data reporting to a shipment tracking center. Two of the studies are particularly notable. Section 1554 of the 9/11 Act requires TSA to develop a shipment tracking program for security sensitive materials consistent with the findings of TSA's Hazmat Truck Security Pilot and to take into consideration the recommendations and findings of FMCSA's Hazardous Materials Safety and Security Technology Field Operational Test in the development of its tracking program.

A summary of each of the Federal studies follows.[1]

FMCSA's Hazardous Materials Safety and Security Technology Operational Field Test[2]

In late 2004, FMCSA completed the Hazardous Materials Safety and Security Technology Operational Field Test, a study to determine if truck telematics technology such as GPS tracking, wireless modems, panic buttons, and on-board computers could be used to enhance hazardous

[1] In addition to the Congressionally-mandated R&D projects, TSA is currently funding the Fedtrak R&D initiative, a project focused on building the software to support an operational Tier 1 HSSM shipment tracking and risk management program.

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

TIER 1 HSSM THREAT SCENARIOS	
Attack Mode	Description
1	Explosive placed on commercial motor vehicle
2	Explosive placed on highway
3	Standoff weapon
4	Vehicle-borne improvised explosive device near commercial motor vehicle
5	Hijacking – immediate release or explosion (outsider threat)
6	Hijacking – release or explosion nearby location (outsider threat)
7	Hijacking – immediate release or explosion (insider threat)
8	Hijacking – release or explosion nearby location (insider threat)
9	Sabotage of TIH cargo tank (release)
10	Initiate Crash

Figure II-4.

materials shipment security. The FMCSA study encompassed all hazmat shipments – a universe of materials much larger than the Tier 1 HSSM universe.

The primary intent of the Hazardous Materials Safety and Security Technology Operational Field Test was to determine the extent to which existing security vulnerabilities in the hazmat supply chain might be reduced by the deployment of truck telematics technology. The study 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 Hazardous Materials Safety and Security Technology Operational Field Test was designed to answer several questions.

Will deployment of truck telematics systems generate security and safety benefits? If so, how much?

What will it cost for hazmat carriers to widely deploy truck- and trailer-telematics systems?

Are the industry operational efficiency benefits generated by the use of telematics systems significant enough to drive widespread industry deployment of truck telematics systems?

FMCSA's Untethered Trailer Tracking Report

FMCSA's Hazardous Materials Safety and Security Operational Field Test includes evaluation of a basic untethered trailer tracking system that provided trailer position and identification information to a dispatcher on a regular basis. However, the House of Representatives Report 107-722, Department of Transportation and Related Agencies Appropriations Bill, directed the FMCSA to conduct further study into untethered trailer tracking (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, geo-fencing, unscheduled movement notification, door sensors, and alarms."

The purpose of the UTT pilot was to develop specific functional requirements that could improve the safety and security of trailers and shipments at each phase of its movement – pick up, delivery, receipt, and storage. The UTT project team developed and tested eight functional requirements: near real-time trailer identification; time of trailer connection and disconnection; trailer location and mapping; geo-fencing; trailer cargo sensing; trailer door sensing; alerts; and software requirements.

FMCSA's Vehicle Immobilization Technologies

In FY 2005, the House of Representatives Conference Report 108-792 directed FMCSA to conduct further testing of truck telematics, including vehicle immobilization.

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.

The purpose of the vehicle immobilization technology (VIT) pilot was to develop specific functional requirements. The project team identified five functional requirements (FRs) of interest for VITs: vehicle disablement if the vehicle senses an unauthorized driver; vehicle disablement/shutdown in the event of a loss of signal; remote vehicle disablement/shutdown by the driver; remote vehicle shutdown by the dispatcher; and remote vehicle shutdown by law enforcement.

FMCSA's Expanded Satellite-Based Tracking System Requirements

In 2004, Senate Conference Report 108-401 pointed out that further commercial motor vehicle tracking capabilities were needed, specifically for shipments of high value goods and hazardous materials traveling through cellular dark zones, and set aside $2 million in funding for a technology pilot program. In the technology pilot program, researchers developed and tested five functional requirements for shipments traveling through remote areas: messaging; location and mapping of tractors; location and mapping of tethered trailers; accurate times of trailer connect and disconnect activities; and panic button alerts.

TSA's Hazmat Truck Security Pilot

FMCSA's Hazardous Materials Safety & Security Operational Field Test first advanced the concept and need for a centralized truck tracking center. TSA's follow-on Hazmat Truck Security Pilot program proved that a centralized truck tracking system – connected to truck-based telematics devices – was feasible. A standards-based XML interface between truck telematics systems and a centralized tracking system was also developed in the TSA Hazmat Truck Security Pilot. However, the technology prototype developed for the pilot program fell far short of what TSA needs in an operational tracking system for Tier 1 HSSM shipments.

The project team evaluated products and services offered by telematics service providers.

The project team conducted a detailed literature review of telematics product/service offerings, followed up by visits to prominent telematics service providers in the United States and Canada.[3] The project team also met with representatives of Singapore's Civil Defence Force (SCDF), Singapore's homeland security agency, to evaluate Singapore's Hazmat Transport Vehicle Truck Security System, a hazmat tracking system that the SCDF implemented to prevent terrorists from using hazmat shipments as weapons.

The purpose of the visits to the telematics service providers was to gather data to support the team's Section 1554 evaluations and to capture the insights of leading telematics service providers on the telematics market. Also, the team was interested in assessing the ability and willingness of the telematics service providers to meet TSA's security needs. Data on technology functionality and telematics system unit costs (capital and operating) was collected by the project team during the visits. While cost and technology data was critical to downstream benefit/cost analyses, information collected during the visits provided the project team with a rich body of qualitative information that also helped the team address a number of pressing programmatic questions facing TSA, including the following.

What telematics functionality should be included in tractor- and trailer-based telematics systems to meet the security challenges facing TSA's highway program? What performance requirements should TSA seek in a telematics system that would meet TSA's Tier 1 HSSM security needs?

How well do the product/service offerings from U.S.-based telematics service providers serve TSA's highway hazmat security needs? Are there gaps? If so, are U.S. telematics service providers willing to invest to refine their product/service offerings to meet TSA needs?

Do the telematics systems offered in other countries incorporate security functionality not offered widely in the United States; especially telematics functionality related to shipment hijacking?

[3] The project team met with the following fleet telematics leaders. **IONX**, West Chester, Pennsylvania; **PeopleNet** (Trimble), Minnetonka, Minnesota; **Qualcomm** (Omnitracs), San Diego, California; **SkyWave**, Ottawa, Ontario; **Teletrac**, Garden Grove, California; **Telogis**, Aliso Viejo, California; **Xata** (XRS), Eden Prarie, Minnesota.

> What are the security benefits of wide-scale deployment of truck telematics systems by Tier 1 HSSM carriers? What will it cost HSSM carriers to deploy telematics systems that satisfy TSA's security needs? Is a regulatory program that requires technology deployment and data reporting to a shipment tracking center justified on a benefit/cost basis?
>
> How should TSA move forward in developing a shipment tracking program that meets the spirit and intent of Section 1554?

Notable findings from discussions with the telematics service providers and SCDF officials follow.

The telematics market has substantially evolved over the past decade. In 2002, when FMCSA began work on its Hazardous Materials Safety and Security Technology Field Operational Test, one telematics firm was dominant – at least in the federal space. However, over the past 10 years, a robust and competitive set of companies has emerged to provide telematics purchasers with more purchasing options, even in the Federal market. While some of the larger telematics service providers offer more choice in terms of hardware/software functionality, most of the major telematics service providers offer similar products and services.

Fleet management systems generate significant cost savings for carriers. Truck telematics systems save carriers money by making their operations more efficient – routing is more efficient, scheduling is more efficient, and less fuel is consumed. Most large, long-haul carriers have already installed truck telematics systems offered from telematics service providers such as Qualcomm and PeopleNet. FMCSA's Hazardous Materials Safety & Security Operational Field Test estimated the unit cost operational efficiency benefits associated with the deployment and use of truck telematics systems. As illustrated in **Figure II-5,** a typical bulk chemicals carrier will save $7,116/truck/year after deploying a basic truck telematics system according to the FMCSA study. An explosives carrier would save $10,968/truck/year. Most bulk chemicals and explosives are Tier 1 Highway Security Sensitive Materials.

Cost reduction from operational efficiency is the key value proposition that telematics service providers offer their customers. Every telematics service providers interviewed by the project team uses a Return on Investment (ROI) sales approach for their telematics/fleet management products and services. Each had compelling data/sales information that proved that their products/services generate very rapid return on investment (ROI) – ranging from a few months to less than a year.

Even though fleet management systems generate compelling ROI, most medium- and small-sized carriers have not deployed truck telematics systems. Almost universally, the telematics service providers complain that many carriers, especially small- to mid-sized carriers refuse to spend the money on telematics even in the face of clear evidence that the investment will pay off quickly in the form of lower operating costs. The upfront cost for purchasing and installing telematics equipment was cited as a major purchasing barrier for small- and mid-sized carriers. All the telematics service providers were in agreement with a conclusion from FMCSA's Hazardous Materials Safety & Security Operational Field Test that only a regulatory driver will prompt wide-scale deployment of telematics systems in any carrier group, including Tier 1 HSSM carriers.

Telematics service providers use a pricing model similar to cellular companies. All the telematics service providers use a pricing model similar to cellular phone companies. For each truck, a telematics service provider will charge an upfront amount to cover the capital cost of the telematics equipment and then a monthly data/communications charge. Like the cellular phone industry, telematics service providers make more of their revenue from monthly data/communications charges than from equipment sales. And like the cellular phone industry, some providers are starting to discount upfront capital costs. For example, Xata (now XRS) is offering a DOT-compliant Electronic On Board Recorder, a basic telematics device, for free. Carriers only pay Xata for monthly EOBR/Hours of Service data services once a Xata EOBR is installed on a truck.

Pricing for tractor-based telematics systems is primarily based on the level of back-end services desired by fleet managers. Telematics service providers sell them services on a tiered basis based on customer preferences. Many telematics service providers their products/services

TELEMATICS AND OPERATIONAL BENEFITS

Operational Benefits	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	$253/month a. $19 b. $122 c. $37 d. $65 e. $11	$491/month a. $30 b. $81 c. $290 d. $78 e. $13
Improved Maintenance Scheduling • Reduces maintenance & repair cost • Increases revenue miles by reducing downtime	$18/month	$37/month
Reduce Out-Of-Route Mile • Creates savings of line haul variable costs	$123/month	$116/month
Improved Vehicle Utilization by Reducing Empty Miles • Increases potential number of trips	$199/month	$270/month
Total Monthly Benefit Per Truck	$593/month	$914/month
Total Annual Benefit Per Truck	**$7,116/year**	**$10,968/year**

Figure II-5.

on an “a la carte” basis – selling only what the customer needs and wants. For example, Qualcomm has three different hardware choices for carriers, including a basic system (MCP 50) for about $450/tractor, and multiple service plans. Qualcomm’s Electronic On-Board Recorder Plan is marketed towards customers that are new to mobile computing and need help staying (or becoming) FMCSA compliant. It gives one access to Hours of Service, basic CSA Safety Performance reporting, vehicle inspection reporting, and basic fleet analytics. Qualcomm’s EOBR plan starts at $19.95 a month/truck.

In a 2010 report, Frost & Sullivan segmented product/services offered by telematics service providers based on functionality, beginning with basic track and trace systems to sophisticated high end fleet management systems.[4] The report also summarized product and service costs by segment as illustrated in **Figure II-6**.

The cost data in Figure II-6 is consistent with the data obtained by the project team during its visits with telematics service providers.

TSA’s Security Action Items have had almost no impact on R&D decisions by telematics service providers, and scant impact on carrier investment. Telematics service providers have not factored TSA’s Security Action Items into product planning and R&D investment, and do not plan to do so until TSA commits to a regulatory program that will require deployment of telematics systems. In their view, regulations drive carrier decisions and voluntary measures like TSA’s Security Action Items have little or no impact on carrier decisions. In fact, the telematics service providers report that there has been little demand from their carrier customers for enhanced security functionality in truck telematics systems. Their customers worry about operational efficiency and compliance with DOT safety requirements. Beyond market demand, market size is a key question for telematics service providers. Telematics service providers will not invest in the research and development needed to refine their products and service offerings to meet TSA security needs in the face of uncertainty over market demand or uncertainty over market size.

It is unlikely that carriers will need high-end fleet management systems to meet TSA security needs. There is a large pricing range for fleet management systems. Capital costs range from $200/unit for basic

[4] Frost & Sullivan, Medium and Heavy-duty Commercial Telematics Life Cycle Analysis of Telematics Services (North America), 2010.

"track and trace" units to over $2,000/unit for high-end fleet management systems. There is also a wide range in monthly service costs as well – ranging from $10/month/truck to $75/month/truck. The telematics service providers were unable to estimate the security hardware/service price point for telematics systems to meet TSA's highway hazmat security needs given the uncertainty over the functionality required. However, in general the telematics service providers felt that TSA's security needs – at least for tractor-based telematics – will be much closer to the low to midpoint of the price spectrum – like DOT's EOBR - than to the higher end, full-service fleet management solutions offered by telematics service providers.

Parsing security data out of the telematics data stream does not represent a technical challenge to telematics service providers. There is no significant technical challenge to telematics service providers in splitting out data flowing from their customers' telematics systems and passing that data onto a central tracking system. The interface with the tracking system needs to be well defined with APIs to support dataflow, however.

Telematics communications have shifted heavily toward cellular. The telematics service providers believed that cellular-based systems would meet the most of the security needs of TSA, even in rural areas. However, at least two telematics service providers pointed out that some customers need hybrid satellite/cellular systems because they travel through remote areas outside of cellular coverage. Also, at least one telematics service provider cited the vulnerability of cellular based systems to jamming/hijacking attacks, and the need for satellite backup capabilities to alert law enforcement officials of attempted hijackings. All the telematics service providers acknowledged that most messaging will flow though cellular systems even when customers use hybrid satellite/cellular systems, and this will mean that the satellite reporting option would be used much less than the cellular option. The cellular-first option provides for more robust and frequent messaging from truck-based systems and much lower operating costs.

Location reporting frequency should be a function of the riskiness of a shipment. The telematics service providers differed in their thinking on appropriate vehicle reporting frequency. In an urban area, the thinking was that location updates would come via cellular networks, a low cost proposition. One telematics service provider said that they normally get two minute location updates but that the reporting rate could be increased if necessary or requested. Another suggested five minutes was a suitable reporting interval. However, the same telematics service provider said that this interval should be contextually dependent upon vehicle type, material type, and location and that an interval of thirty seconds was a good value for exigent circumstances (when there is high risk/high threat).

Mobile/hand-held devices are becoming more sophisticated; offer better telematics options. Telematics service providers are investing more heavily in mobile/hand-held devices in conjunction with their truck telematics systems. Hand-held devices include smart phones and hand-held terminals/computers. DOT's EOBR/HOS rule

OPERATING COST OF TELEMATICS SYSTEMS

	Track and Trace System	EOBR/Hours of Service	Entry Level Fleet Management System	Mid-Level Fleet Management System	High End Fleet Management System
	Collection of basic vehicle location data for tracking and back-end report generation	Stand-alone remote vehicle diagnostics + basic track & trace	EOBR plus basis Fleet Management System (FMS)	Entry level plus navigation services and additional FMS applications	Mid-Level plus advanced vehicle/driver applications, advanced logistics management
Hardware Cost Range ($/tractor)	$200 - $300	$0 - $350	$500 - $750	$1,0000 - $1,500	$1,500 - $2,300
Service Cost Range ($/tractor/month)	$10 - $20	$20 - $30	$25 - $35	$35 - $45	>$45

Figure II-6.

has been particularly influential in pushing the market toward hand-held devices. This move also corresponds to increased computing/processing power on devices at the truck level. Enhanced processing at the truck level lessens messaging volume/frequency with telematics service providers' back end data services.

Insurance telematics has been a positive influence in the fleet safety market. Some insurance companies require carriers – especially carriers with problematic safety records – to install telematics systems and monitor driver behavior. Industry studies have found that driver behavior improves substantially when drivers know that their driving performance will be continually monitored and that fleet managers will have access to driver reports. In turn, this reduces safety vulnerabilities across a carrier fleet. Carriers also realize lower operating costs. One telematics service provider estimates that telematics can give carriers a 12% productivity increase and a 12-15% reduction in fuel consumption as a result of recording and rooting out poor driver behaviors like driving over 65 mph and hard acceleration.

Hijacking is a serious issue in other countries, and telematics systems have evolved to counter the threat. Hijacking, theft by diversion and insider attacks are more commonplace in other countries, particularly for shipments of high value goods. Increasingly, hijackers are using GPS/GSM jammers to overwhelm truck telematics systems during a hijacking attempt. The trucking telematics industry has evolved to meet the security threats in these countries. For example, on-board systems have been physically hardened and anti-jamming functionality has been built into telematics devices. For example, a Canadian telematics hardware manufacturer offers telematics hardware that incorporates anti-jamming functionality to detect and defeat hijacking attempts. This hardware is used throughout the world including the Brazilian and Mexican markets. A South African telematics service provider offers a system that allows security operators to covertly monitor (via audio) a truck's cab to determine if a shipment has been compromised by hijackers. The same system allows the driver to establish an audio bridge to the back-end security office with the press of a button. In Brazil, carriers of high value goods often use multiple (redundant) telematics systems and antennas on a single truck, and place telematics devices on (and in) vehicles to prevent them from being easily detected and decommissioned. While HSSM shipment hijacking is a threat that concerns TSA, U.S. telematics service providers have been slow to introduce telematics offerings to address the threat, citing low demand by U.S. carriers.

Trucking security standards issued by Transported Asset Protection Association (TAPA) in late 2011 address security scenarios of concern to TSA. The U.S. telematics industry is lagging behind other countries when it comes to security innovations, but there is growing interest in protecting high value goods shipments. The International Organization for Standardization (ISO) issued ISO 28000, "Specification for Security Management Systems for the Supply Chain," to support the need for enhanced supply chain security. The Transported Asset Protection Association (TAPA) issued trucking security standards based on ISO 28000 in late 2011. The TAPA standards are relevant to a number of the HSSM security scenarios facing TSA, and directly address a number of issues related to truck telematics technology choices and system functionality requirements for these scenarios.

Systems that prevent unauthorized drivers from starting and driving a truck are lightly deployed in the United States but are on the upswing. The use of driver authentication systems that prevent an unauthorized driver from starting a truck are on the upswing in the United States, especially as industry organizations such as the Transported Asset Protection Association (TAPA) have become more active in response to hijacking threats to high value goods shipments.

Systems that disable moving vehicles are rarely deployed, even though disabling functionality is offered by U.S.-based telematics service providers. 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. The use of driver authentication systems that prevent an unauthorized driver from starting a truck is on the upswing in the United States, especially as industry organizations such as the Transported Asset Protection Association (TAPA) have become more active in response to hijacking threats to high value goods shipments. However, systems that allow dispatchers or fleet managers to disable a moving vehicle are lightly or rarely deployed in the U.S.

Singapore's Hazmat Transport Vehicle Tracking System incorporates vehicle disabling technology. In July 2005, Singapore began operating its Hazmat Transport Vehicle Tracking System (HTVTS), the world's first hazmat transportation security system. The HTVTS 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. As of April 2007, the SCDF required hazmat carriers to upgrade their on-board telematics hardware with an immobilizer device. SCDF's immobilization device controls the throttle limiters that restrict the fuel injection to prevent acceleration and limit throttle response. This slows a vehicle progressively without interfering with its power steering and braking system. Once the immobilizer is activated, a vehicle will slow 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 an eventual stop.

SCDF offered TSA and the project team lessons learned from implementing its truck tracking program. Singapore is a city-state. While densely populated, its land area is no larger than most mid-sized U.S. cities. The SCDF built its hazmat regulatory program and the Hazmat Transport Vehicle Truck Security system to serve Singapore's unique city-state security, business, and regulatory environment. The HTVTS functions well in Singapore's single-city, highly-regulated environment where there are a small number of shipments, where trip lengths are very short, and where routing and equipment choices by carriers can be tightly controlled. The HTVTS will not satisfy U.S. security, business, and regulatory needs, however. The U.S. transportation network is huge in relation to Singapore's network and HTVTS functionality falls far short of what TSA needs in a Tier 1 HSSM SAI-compliant truck tracking system. Also, the HTVTS will not support the complex relationships between TSA, industry, states, and other government agencies that need to be served in the U.S.

There are, however, lessons TSA can draw from Singapore's experience in building and operating the HTVTS. For example, SCDF officials stressed to TSA and the project team that vehicle disabling is critical in an urban, target-rich area like a High Threat Urban Area. SCDF officials believe that the value of a truck security program would be greatly diminished if officials cannot stop a truck in the hands of a terrorist before it reaches a high value target. Other SCDF lessons learned from its HTVTS experience are presented in **Sidebar 3**.

DOT's EOBR/Hours of Service requirements are driving telematics investment by commercial vehicle operators. Longstanding DOT regulations set detailed and specific requirements that limit the hours of service that a driver can remain on-duty without rest, and require drivers to maintain a log recording their hours of service. For years, drivers kept paper log books, known as the driver's "record of duty status" to track their hours of service. DOT's EOBR rule, as mandated under MAP-21, will require carriers to install EOBRs to replace paper log books. EOBRs must meet minimum functional requirements, including the ability to integrate with a tractor's engine/sensor (JBUS) network, to identify the vehicle's driver, and to report out vehicle location. While the telematics functionality in DOT's EOBR will not fully meet TSA's needs, JBUS integration and GPS/location reporting are both core functions that TSA needs in a telematics security solution. Telematics service providers are excited about DOT's EOBR/hours of service rule. Originally, DOT planned to require only carriers with poor safety scores to deploy EOBRs. The latest rule will require many more carriers (including virtually 100% of HSSM carriers) to deploy EOBRs by 2015. This represents a tangible growth opportunity for telematics service providers. Every U.S.-based telematics service provider interviewed by the project team already offers an EOBR in their product/service lineups and all are looking to final DOT requirements to refine their products to support DOT's EOBR/hours of service requirements. EOBR/hours of service competition between U.S. telematics service providers will be strongest for medium-sized carriers that will install telematics systems for the first time or plan to upgrade telematics functionality beyond basic "track and trace".

More information of DOT's EOBR/hours of service requirements may be found in **Annex B**.

DOT's EOBR experience reinforces earlier findings about carrier behavior; argues for regulations to drive telematics deployment. FMCSA's Hazardous Materials Safety & Security Operational Field Test concluded that the majority of hazmat carriers would not deploy truck telematics systems in the absence of a regulatory requirement to do so – even though truck telematics systems generate significant cost savings for carriers.

> *"… 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."*

In a related issue, the FMCSA study also concluded that the highway hazmat security program would fail without widescale technology deployment.

Singapore Civil Defence Force Hazmat Transport Vehicle Tracking System — Lessons Learned

Regulations have to drive technology deployment. The SCDF considered a voluntary call for installation of telematics technology but found that a few good corporate citizens would deploy tracking systems and submit tracking data to the SCDF but 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 to its tracking center.

Regulations and technology have to be in alignment. A regulatory program that outreaches what is possible from a technology perspective will fail. The SCDF carefully tailored telematics 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. 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 has a robust compliance program to ensure high compliance by hazmat carriers. According to the SCDF, a weak compliance program will be quickly exploited.

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 some 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.

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.

SIDEBAR 3.

> *"It should be noted that partial deployment might not necessarily result in a directly proportional security benefit. In other words, 50 percent deployment may not yield 50 percent of achievable security benefits. This may occur because while the technology-equipped fleet may not be attacked, a non-equipped fleet would possibly be targeted instead. The deterrent effect of the technologies, if partly deployed, could simply shift terrorist targeting from one fleet to another, with no net change in overall security. Under this assumption, then full deployment is required to realize the security benefits."*

DOT's experience from its recent EOBR/Hours of Service initiative reinforces conclusions reached in FMCSA study. DOT found that many commercial motor carriers will not deploy EOBRs or truck telematics systems unless regulations require them to do so, even if telematics deployment generates substantial cost savings for carriers as numerous public and private studies have shown. Also, DOT's experience proves that telematics service providers will not invest internal research and development funds to refine their products and services to meet a government requirement unless that requirement is rooted in a regulation that provides the telematics service providers certainty over market size and functionality requirements.

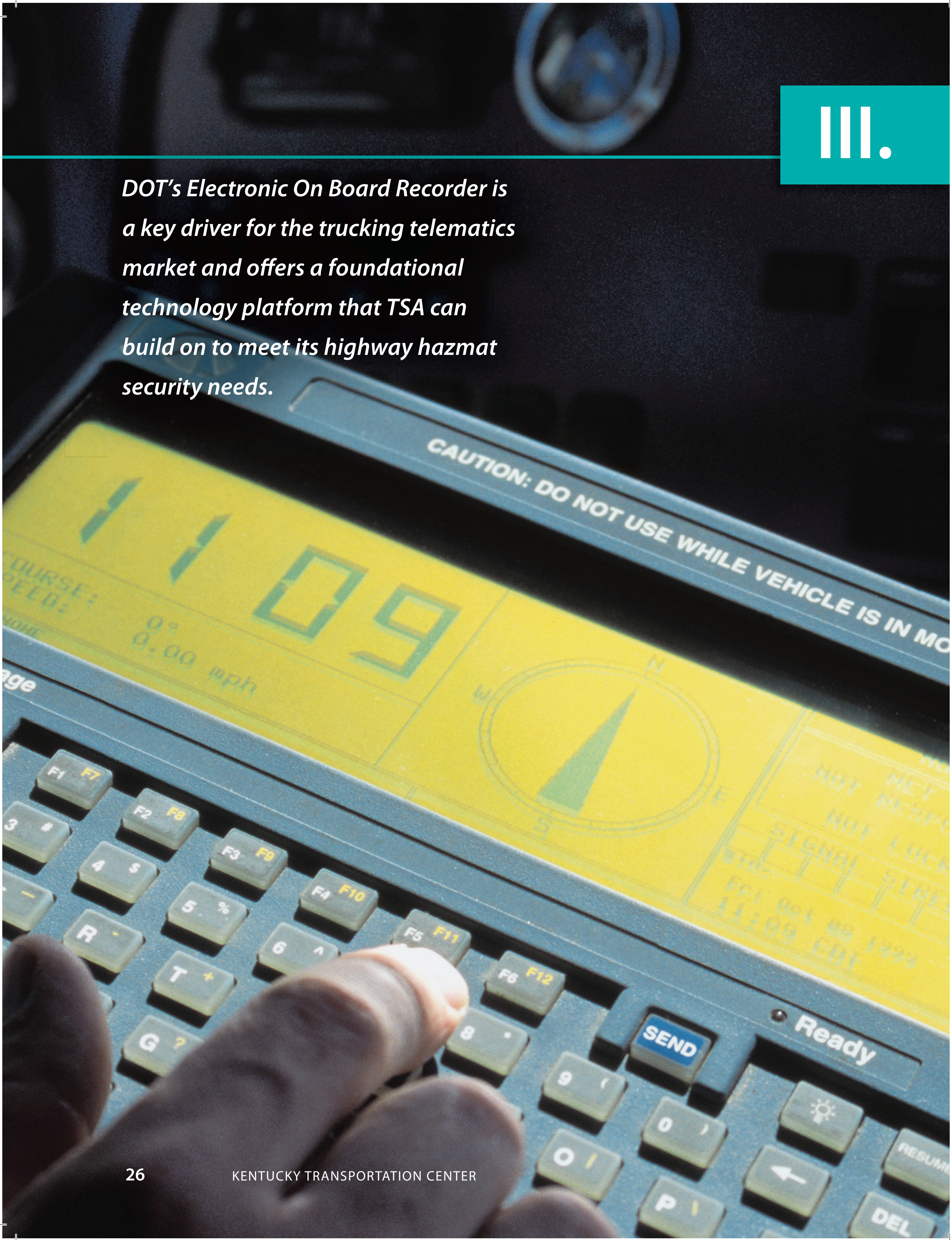
DOT's EOBR performance/data standards guide telematics service providers. In its original EOBR 1 rule, DOT advanced a "technology bar" for EOBRs that requires, among other things, that EOBR technology (1) identify the driver prior to transit, (2) track the time when the driver is actually driving, (3) record the location of the vehicle as it moves, (4) record identifying details about the truck, (5) record details about the shipment being carried, and (6) and be capable of sharing collected data according to structured data elements and via wired and wireless methods. In general, telematics service providers are comfortable with technology and data performance requirements and all the telematics service providers interviewed in this project have refined their existing products/services in order to offer EOBR/hours of service support to their customers. **Figure II-7** highlights some of the key EOBR performance standards and data sharing standards as required by EOBR I. **Annex B** provides additional information on DOT-proposed EOBR data reporting and data sharing performance standards.

DOT EOBR TECHNOLOGY PERFORMACE STANDARDS	
Automatically Record Driving Time and "Duty Status"	• Must automatically record driving time when vehicle is in motion.
Driver Identification and Login	• Must require a user id/password, or other means such as smart cards or biometrics to identify the driver.
Record Vehicle and Shipment Information	• Must record USDOT Number of motor carrier. • Must record the truck number or tractor and trailer numbers. • Must record the shipping document number(s), or name of shipper and commodity.
Track Location of Vehicle	• While in motion, must record location at a maximum of 60-minute intervals. • During "duty status" change, must record location of nearest city, town, or village. • Location of vehicle must be derived from satellite or terrestrial sources, or a combination of both. • Must record distance traveled during on-duty driving period.
Display Functions	• Must have the capability of displaying a variety of enumerated information, including driver name, driver ID, total hours on duty, miles driven and additional data.
Performance Features	• Must give audible and visible signal when driver nears driving time limit • Must give audible and visible signal if device loses its communication signal for more than brief periods • Must allow for driver input of data only if vehicle at rest • Must not permit alteration or erasure of data collected by the EOBR
Self-Certification	• Manufacturer must self-certify EOBR as meeting the requirements of the regulation.

Figure II-7.

III.

DOT's Electronic On Board Recorder is a key driver for the trucking telematics market and offers a foundational technology platform that TSA can build on to meet its highway hazmat security needs.



TELEMATICS AND TIER 1 HSSM SHIPMENTS FINDINGS & RECOMMENDATIONS

As noted in the preceding section, DOT will require almost all commercial motor vehicles to deploy an Electronic On Board Recorder (EOBR) by late-2015 under its EOBR/hours of service rule. Under the rule, carriers must install EOBRs that meet minimum functional requirements, including the ability to integrate with a tractor's engine/sensor network, to identify the vehicle's driver, and to report out vehicle location. Essentially, an EOBR is a basic telematics device. While the telematics functionality in DOT's EOBR will not fully meet TSA's security needs, JBUS integration and GPS/location reporting are both core functions that TSA needs in a telematics security solution.

The project team recommends that TSA leverage DOT's EOBR initiative by enhancing the basic telematics functionality in DOT's EOBR so that it can operate as a combined safety and security EOBR for deployment by Tier 1 HSSM carriers. This **Security EOBR** would not only have the functionality to meet DOT's Hours of Service needs, but would include extra functionality to meet TSA's security needs for Tier 1 HSSM carriers.

Using DOT's EOBR as a foundational telematics platform offers TSA and the carrier community a number of advantages.

Consistency with Section 1554 collaboration mandate. Section 1554 requires TSA to consult with DOT as it develops its shipment tracking program. Development of the Security EOBR will bring TSA and DOT telematics initiatives into close alignment, meeting the spirit and intent of Section 1554.

Shared data/performance standards. DOT has done a great deal of work in defining data standards and in developing performance standards for its EOBR/Hours of Service program. By leveraging this work, TSA can not only achieve programmatic consistency but also substantially reduce its burden in developing its security telematics solution. Tier 1 HSSM carriers – jointly regulated by DOT (safety) and TSA (security) – will also benefit from a single, comprehensive set of data and performance standards.

Simpler telematics solution; leverage investment by telematics service providers. The Security EOBR will satisfy a Tier 1 HSSM carrier's Hours of Service (safety) and security requirements with a single telematics unit instead of separate safety and security devices, lowering capital costs. Also, carrier operating costs, especially communications costs, will be lower in a combined telematics solution. Telematics service providers can leverage existing EOBR/HOS software investment by integrating safety and security applications in a combined EOBR.

The project team approached its analysis of TSA's telematics needs by beginning with DOT EOBR telematics functionality as a baseline, and then determined what incremental functionality would be needed for TSA's highway hazmat security program. Specific threat scenarios facing the highway hazmat security program such as those listed in Figure II-4 were evaluated in terms of telematics functionality requirements, and the project team examined telematics systems used in other countries in terms of their security functionality, especially functionality related to the threat of hijacking. The project team also evaluated the event/messaging requirements that would be needed in TSA's security program versus those that support DOT's safety program as well as specific technology issues called listed in Section 1554(a)(2)(c). The end result was development of functionality requirements for the Security EOBR.

The project team evaluated specific telematics technology issues identified in Section 1554.

Section 1554(a)(2)(c) requires TSA to focus on three specific telematics technology issues:

Section 1554(a)(2)(c)(ii) - the ability of tracking technology to resist tampering and disabling;

Section 1554(a)(2)(c)(iv) - the appropriate range of contact intervals between the tracking technology and a commercial motor vehicle transporting security-sensitive materials; and

Section 1554(a)(2)(c)(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.

The project team evaluated these three technology issues as it crafted recommendations for telematics functionality for the Security EOBR.

GPS Spoofing and Truck Telematics

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory conducts multi-disciplinary research and development on physical security devices, systems and programs.

In 2002, the VAT conducted a study focused on determining if it could defeat existing truck telematics security systems used in the transport of sensitive materials in a hypothetical truck hijacking. At the time, the use of GPS for security and cargo tracking was gaining in popularity with the idea that if a vehicle is stolen, the tracking device on the vehicle would report its exact location to authorities. In the back-office monitoring center, tracking information for a given vehicle would be displayed and if the vehicle deviated from its intended route by more than some preset limit, an alarm would sound.

The VAT team came up with an attack strategy, GPS spoofing, to defeat the prevailing security assumptions. In a GPS spoofing attack, the adversary controls the signal that the truck is receiving. A false position calculated by the receiver is relayed to headquarters regardless of the encryption algorithms or communication protocols used.

Using inexpensive and commercially available components, the VAT proved that truck telematics systems were vulnerable to GPS spoofing, and that a determined hijacker could not only hijack a truck but prevent authorities from discovering that the attack had even occurred until well after the attack had transpired. The overall VAT conclusion:

> *"Although this demonstration can hardly be considered a thorough or rigorous vulnerability assessment, it certainly does suggest that civilian GPS is indeed vulnerable to simple spoofing attacks that almost anyone could exploit.* ***Simply because GPS is high technology does not mean it offers high security."***

Argonne
NATIONAL LABORATORY

SIDEBAR 4.

SECTION 1554(2)(C)(II) TAMPERING AND DISABLING

There are two ways to disable tractor-based or trailer/tanker-based telematics systems: 1). physically disabling the system by tampering with wiring and/or telematics hardware; or 2). remotely disabling/blocking the GPS and or GSM functionality of the telematics system using non-physical means.

A telematics system can be easily defeated if wiring or hardware components, especially antennas, are visible and unprotected. Cutting exposed wiring or ripping a GPS antenna off a truck will disable a vehicle telematics systems by "blinding it" to GPS satellite signals. Also, disabling a GSM/cellular system by cutting exposed wiring or ripping the GSM antenna off the truck will prevent the truck's telematics system from "communicating" via a cellular network with the back end operations center.

Originally used in military applications to confuse enemy navigational systems, GPS signal jammers are becoming common tools used by thieves, especially in countries such as Brazil where truck hijacking is a significant problem. GPS jammers interfere with the operation of on-board GPS chips in navigation and tracking devices, allowing thieves to steal trucks and cargo while leaving fleet managers and police unable to quickly detect that the truck has been stolen or its location.

A more sophisticated version of GPS jamming is GPS spoofing in which an adversary replaces the GPS signal from the truck to the telematics operations signal with a false signal that presents the truck at different location than where it actually is. In 2002, the Vulnerability Assessment Team, now located at Argonne National Laboratory, proved that shipments of sensitive materials were vulnerable to hijackers using GPS spoofing attacks.[1] **Sidebar 4** describes the field test conducted by the Vulnerability Assessment Team.

Like GPS jammers, GSM jammers are also readily available. GSM jammers block or overwhelm GSM signals and prevent

[1] The Vulnerability Assessment Team was located at Los Alamos National Laboratory at the time of the GPS spoofing test.

cellular-based tracking devices from sending position information and theft alerts. GSM jammers can also prevent drivers from using their cell phones to communicate.

Figure III-1 summarizes the two types of attacks – physical and non-physical – that are used to disable truck-based and trailer/tanker-based telematics systems.

The U.S. telematics industry is lagging behind other countries when it comes to security innovations. Installations of telematics systems in other countries are routinely "hardened" to resist physical attacks. Also, "anti-jamming" GPS chips used in tractor-based telematics systems are programmed to detect and warn against GPS and GSM jamming attacks. Section III touched on telematics systems offered in other countries that incorporate "anti-jamming" GPS chips into telematics black boxes to combat hijacking of high value goods shipments.

In late 2011, the Transported Asset Protection Association (TAPA), which includes representatives from major U.S. firms in the pharmaceutical, electronics, and consumer goods industries, issued trucking security standards based on ISO 28000, "Specification for Security Management Systems for the Supply Chain". The TAPA trucking security standards are relevant to a number of the HSSM security scenarios facing TSA, especially shipment hijacking, and directly address a number of issues related to truck telematics technology choices and system functionality requirements. TAPA's trucking security standards serve as the basis for an audit/certification program used by TAPA-affiliated companies.

The project team recommends the following in regards to tampering/disabling and TSA's highway hazmat security program.

1. The Security EOBR should detect and report trailer/tanker untethering (disconnects) for Tier 1 HSSM shipments between gate-out and gate-in.

2. The trailer-based telematics system should detect and report trailer door opening and open/close door status between shipment gate-out and gate-in. Likewise, a tanker-based telematics system should detect and report hatch opening and open/close hatch status.

3. The Security EOBR should detect a GSM/GPS jamming attack and send an alert message to the shipment tracking center, the carrier, and to the driver. This means the Security EOBR should incorporate a GPS chip programmed to detect a jamming attack and a hybrid satellite/cellular modem that is capable of sending a message to the shipment tracking center (and to continue location reporting) if the vehicle's cellular network has been compromised by jamming.

4. Telematics hardware - including cables, wires, terminals, antennas, on-board computers - should be secured against attempts to defeat them by physical means, both on the tractor as well as trailers/tankers. TSA should adopt regulations/standards for the physical security of Tier 1 HSSM truck/trailer-based telematics systems at least as stringent as those for high value goods shipments.

PHYSICAL/NON-PHYSICAL ATTACKS TO DISABLE GPS/GSM TELEMATICS SYSTEMS		
Physical	In this attack, an adversary physically disables the telematics systems by ripping out wiring to GPS/GSM antennas or by ripping down GPS/GSM antennas, preventing the telematics system from communicating with the telematics operations center. Similarly, the adversary can attack other hardware components of the system.	
Non-Physical	GPS/GSM Jamming	In this attack, an adversary uses a jamming device to overwhelm the GPS receiver by filling the GPS bandwidth of frequency with energy, causing the GPS receiver to lose lock on GPS satellites or never attain lock. This type of attack is sometimes referred to as denial of service. Very inexpensive portable jammers – easily built from readily available commercial components - have been used by criminal gangs to jam truck telematics systems during hijacking attempts.
	GPS Spoofing	Automatically Record Driving Time and "Duty Status"

Figure III-1.

5 TSA should adopt requirements for covert installation of telematics hardware for vehicles carrying Tier 1 HSSMs at least as stringent as TAPA's Trucking Security Requirements (TSR) for high value goods shipments. Also, TSA should adopt a requirement for trailer door and tanker hatch locks at least as stringent as TAPA's Trucking Security Requirements (TSR) for high value goods shipments.

SECTION 1554(2)(C)(IV) CONTACT INTERVAL RANGE

Over the past 15 years, telematics technology has trended toward cellular (or hybrid cellular/satellite) telematics systems and away from satellite-only telematics systems. The cost of location/event reporting over a cellular network is low compared to reporting over a satellite system, fostering significantly higher reporting rates and expanded over-the-air message sets.

The project team searched out "benchmarks" for location and event reporting including a review of FMCSA's Hazardous Material Safety and Security Operational Field Test, TSA's Hazmat Truck Security Pilot, current DoD and DOE shipment tracking programs, and DOT's EOBR/Hours of Service program. The project team also reviewed tracking/security programs in other countries in its benchmarking effort.

The project team recommends the following in regards to contact intervals and TSA's highway hazmat security program.

1 The shipment tracking center needs to be able to "interrogate" a Security EOBR at any time on a machine-to-machine (M2M) basis to determine the real-time location of a shipment of Tier 1 HSSMs. This means that security personnel at the tracking center must be able to "ping" the Security EOBR installed on a tractor at any time to get its location.

2 **Figure III-2** lists events that a Security EOBR should automatically report to the shipment tracking center as the event occurs. An event report will include an event code, the telematics unit identification number, the location where the event occurred (latitude/longitude), and time the event occurred.

3 Security EOBRs will report events as they occur, however, location reporting rates will vary depending on the tractor's location and its security status. In general, the triggers for variable reporting are as follows.

A security incident will require increased location reporting.

Travel in or close to a High Threat Urban Area will require increased location reporting.

Travel in a cellular dark zone will require location reporting via a satellite network, but at a reduced reporting rate.

For Tier 1 HSSM shipments traveling through TSA-designated High Threat Urban Areas (HTUAs), the project team recommends that Security EOBRs be programmed to report location to the shipment tracking center once/minute, the same location reporting standard used by the Singapore Civil Defence Force for trucks traveling on Singaporean roads. Location reporting will increase to every fifteen seconds in the event of a security incident. Note that

[2] A High Threat Urban Area (HTUA) is an area comprising one or more cities and surrounding areas including a 10-mile buffer zone. There are about 50 TSA-designated High Threat Urban Areas.

[3] A "No Drive Zone" is a special type of geofence. The telematics device on vehicle carrying Tier 1 HSSMs will automatically disable the vehicle if it enters a TSA-designated no drive zone. See following section on Vehicle Disabling.

REPORTABLE EVENTS – SECURITY EOBR (TRACTOR-BASED TELEMATICS UNIT)		
Shipment Gate-Out (shipper location)	Shipment Gate-In (consignee location)	Panic Button Alert
Rest In/Out	Vehicle Stop	Stop Greater Than (TBD) Minutes
Ignition On or Off (state change)	Equipment Tampering Alert	Trailer/Tanker Disconnect Alert
Exit State (border cross)	Enter State (border cross)	Impact, Accident, Roll Over Alert
Enter High Threat Urban Area[2]	Exit High Threat Urban Area	Enter Cellular Dark Area
Exit Cellular Dark Area	Begin GPS Jamming	End GPS Jamming
Outgoing Call to Tracking Center	Incoming Call from Tracking Center	Enter No Drive Zone[3]
Disable Signal Received		

Figure III-2.

cellular networks will be readily available in the HTUAs – thus making it a rare event that reporting will need to be made over the more costly, backup satellite system. **Figure III-3** summarizes the project team's recommendations for Security EOBR tractor location reporting.

4 Two-way machine-to-machine (M2M) messaging between the Security EOBR and the shipment tracing center is needed to support vehicle disabling, location polling, variable location reporting, and event reporting. The Universal Communications Interface (UCI) developed during TSA's Hazmat Truck Security Pilot was built assuming there would be only one-way messaging – from a telematics service provider to the shipment tracking center. Two-way M2M messaging between the tracking center and the Security EOBR is needed to provide TSA the security functionality it needs, especially in terms of managing reporting frequency and in managing communications during a security incident. For example, TSA will require more frequent location reporting for a shipment in a High Threat Urban Area than a shipment well outside the HTUA. The UCI will need to be re-engineered to support M2M messaging. Also, tracking center systems may direct the Security EOBR on a tractor to increase location reporting if the shipment is off route.

5 Trailers and tankers will have telematics systems separate from tractor-based systems, and different location/event reporting requirements. In general, a heavier reporting burden should be placed on the Security EOBR than trailer/tanker-based systems. Trailer/tanker-based systems are usually battery-powered, unlike tractor-based systems, and battery life preservation is important. Also, location reporting from trailers/tankers is less important when they are paired with a tractor. Location reporting becomes important when a trailer or tanker is unexpectedly disconnected from a tractor between gate-out and gate-in indicating the possible theft or diversion of HSSMs. **Figure III-4** lists events that a trailer-based telematics system should automatically report to the shipment tracking center.

6 **Figure III-5** summarizes the project team's recommendations for trailer/tanker location reporting frequency. Note that the project team expects almost all location reporting will take place over cellular networks.

The shipment tracking center may increase trailer location reporting in the event of a security incident, especially if the trailer is unexpectedly disconnected from the tractor. The shipment tracking center will direct the trailer's telematics system to increase location reporting frequency on a machine-to-machine basis.

RECOMMENDED TRACTOR LOCATION REPORTING FREQUENCY – SECURITY EOBR

Location Report Trigger	Tractor Reporting Frequency Cellular System Available	Tractor Reporting Frequency Cellular Dark Zone
> 50 miles from HTUA, no incident	30 minutes (with 1 minute breadcrumbs)	Upon entry into active cellular coverage area or 60 minutes (with 1 minute breadcrumbs)
25-50 miles from HTUA, no incident	15 minutes (with 1 minute breadcrumbs)	Upon entry into active cellular coverage area or 20 minutes (with 1 minute breadcrumbs)
<25 miles from HTUA, no incident	5 minutes (with 1 minute breadcrumbs)	Upon entry into active cellular coverage area or 10 minutes (with 1 minute breadcrumbs)
In HTUA, no incident	1 minute	1 minute
Within 5 miles of No Drive Zone, no incident	1 minute	1 minute
Incident-type event outside HTUA	30 seconds	1 minute
Incident-type event in HTUA	15 seconds	30 seconds

Figure III-3.

SECTION 1554(2)(C)(V) - VEHICLE DISABLING

The project team reviewed research conducted by FMCSA on vehicle disabling systems and investigated disabling systems that have been deployed in other countries. Singapore's experience in implementing its Hazmat Transport Vehicle Tracking System is particularly instructive in relation to TSA's security needs in and around TSA-designated High Threat Urban Areas.

Driver authentication systems that prevent unauthorized drivers from starting and driving a truck are lightly deployed in the United States even though the technology is readily available. However, the use of these driver authentication systems is on the upswing in the United States, especially as industry organizations such as TAPA have become more active in response to hijacking threats to high value goods shipments. The project team recommends that Tier 1 HSSM tractor-based telematics systems include driver authentication functionality.

Systems that disable moving vehicles are rarely deployed in the United States. Singapore's Hazmat Transport Vehicle Tracking System operated by the Singapore Civil Defense Force (SCDF), the country's homeland security agency, has employed vehicle disabling as a core feature since 2007. If a truck carrying hazardous materials strays from an authorized route in Singapore, immobilization controls in the truck telematics system restrict the fuel injection to prevent acceleration and limit throttle response. This slows a vehicle progressively without interfering with its power steering and braking system. Once the immobilizer is activated, a vehicle will slow safely to a low speed of 10km/hour to enable the driver to maneuver it to the side of the road before it comes to an eventual stop. SCDF officials also have the option of remotely disabling a vehicle.

In interviews with the project team, SCDF officials argued that vehicle disabling is critical in an urban, target-rich area like a High Threat Urban Area. They believe that the value of a truck security program would be greatly diminished if officials cannot stop a truck in the hands of a terrorist before it reaches a high value target.

The project team recommends the following in regards to vehicle disabling and TSA's highway hazmat security program.

1 The Security EOBR should have the capability to allow a carrier to remotely disable a tractor hauling Tier 1 HSSMs upon direction by TSA and/or authorized state or local law enforcement agency.

EVENT -BASED REPORTING – TRAILER/TANKER

Trailer/tanker connect (at shipper location)	Trailer/tanker disconnect (after gate-in at consignee location)	Trailer/tanker disconnect (between gate-out and gate-in – potentially represents the initiation of a security incident)
Hatch (tanker) or door (trailer) close (at shipper location before gate-out). Hatch (tanker) or door (trailer) open (at consignee location) after gate-in.	Hatch (tanker) or door (trailer) open (between gate-out and gate-in – potentially represents the initiation of a security incident)	Impact, accident, or roll over (represents the initiation of a safety or security incident)

Figure III-4.

RECOMMENDED TRAILER/TANKER LOCATION REPORTING FREQUENCY

Location Report Trigger	Tractor Reporting Frequency Cellular System Available	Tractor Reporting Frequency Cellular Dark Zone
Outside HTUA	60 minutes (with 15 minute breadcrumbs)	Upon entry into active cellular coverage area or 60 minutes (with 15 minute breadcrumbs)
Inside HTUA	5 minutes	15 minutes
Incident	TBD	TBD

Figure III-5.

2 A Tier 1 HSSM driver should not be able to start or drive a truck hauling HSSMs without authenticating his/her identity using the Security EOBR.

3 The Security EOBR should have the capability to automatically disable a tractor when that tractor enters a No Drive Zone established by TSA.

4 The Security EOBR should have the capability to allow TSA and/or an authorized state/local law enforcement agency to remotely disable a tractor hauling Tier 1 HSSMs. The Security EOBR should be able to accept a disabling message – from the carrier, law enforcement agency, or TSA – via cellular and satellite networks.

The Security EOBR will meet TSA's highway hazmat security needs as well as DOT's Hours of Service needs.

As noted earlier, the project team recommends that TSA leverage DOT's EOBR initiative by enhancing the basic telematics functionality in DOT's EOBR so that it can operate as a combined safety and security EOBR for deployment by Tier 1 HSSM carriers. The project team approached its analysis of TSA's telematics needs by beginning with DOT EOBR telematics functionality as a baseline, and then determining what incremental functionality would be needed for TSA's highway hazmat security program. **Figure III-6** is a pictorial representation of the Security EOBR in-cab terminal. **Figure III-7** further describes the Security EOBR and the incremental security functionality that would be embedded in it. The Security EOBR will build on data standards and event-based messaging developed by DOT for its EOBR/Hours of Service program (refer to Figure IV-9). For example, the Security EOBR would be programmed to support a deeper set of event-based messages to meet TSA's highway hazmat security needs than those needed to meet DOT's Hours of Service program. **Annex B** describes DOT's EOBR and data/performance standards developed by DOT for its Hours of Service program.

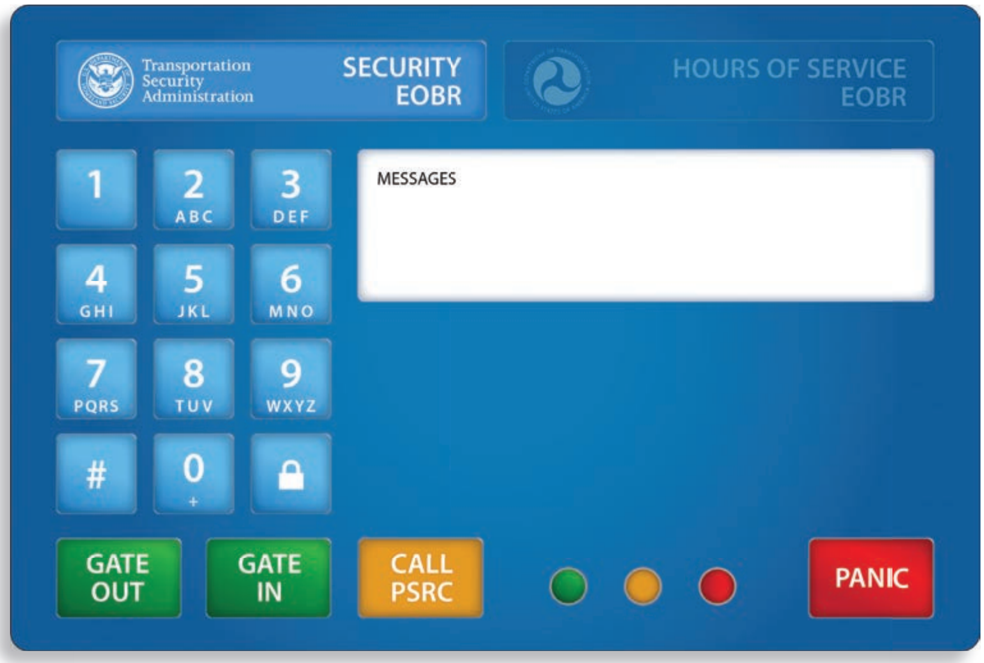


Figure III-6. Security EOBR In-Cab Terminal

SECURITY EOBR (TRACTOR-BASED TELEMATICS SYSTEM)			
In-Cab Terminal		Panic Button	Panic button functionality was a key security feature cited in both FMCSA's Hazardous Materials Safety & Security Operational Field Test and in TSA Security Action Items. The in-cab terminal should prominently display a panic button that the driver can push to send an alert to the shipment tracking center, triggering immediate attention by Security Specialists at the shipment tracking center.
		Tracking Center Push to Talk Button (over-the-air audio communications) Microphone and Speaker	Beyond the Panic Button, the in-cab terminal should include a button that – when pushed by the driver – will establish a direct audio bridge to a Security Specialist at the shipment tracking center. The driver can connect with the tracking center with issues that fall short of an emergency that necessitates the use of the Panic Button. The functionality embedded in the in-cab device will also allow Security Specialists to directly contact to the driver if there is a security concern and/or to covertly monitor (via audio) a truck's cab to determine if a shipment has been compromised by hijackers or if the driver is in distress. This functionality is similar to the audio bridge functionality in the South African telematics system described in Section II except that the audio bridge is between the driver and the shipment tracking center.
		Gate-Out Button Gate-In Button	A Tier 1 HSSM driver will push the "gate-out" button on the in-cab display when the driver leaves a shipper's location. Likewise, the driver will push the "gate-in" button on in-cab terminal device when the driver arrives at the consignee's location. The gate-out event signals the shipment tracking center that the shipment is "live" and on the road. The gate-in event signals the shipment tracking center that the shipment has arrived safely at the consignee's location. On a software basis, gate-out and gate-in event messages will be integrated with electronic manifest business processes.
		Text Display	Provides short text messages such as error display messages or text messages from the shipment tracking center.
		Indicator Lights	The (red, green, yellow) indicator lights on the in-cab display will be programmed to give the driver various visual cues. For example, the green light might be programmed to indicate that the shipment tracking center has received the signed electronic manifest, and the driver is free to leave a shipper's location with the Tier 1 HSSM load.
		Keypad (driver log-in and authentication)	The keypad supports driver authentication. A driver cannot start the truck without entering in a driver-specific code. (Note that driver authentication will be integrated with the EOBR/HOS driver login on a software basis.)
On-Board Computer and Other Hardware/Software Components		On-Board Computer (black box)	The on-board computer connects to the in-cab terminal with wiring and is wired into the tractor's J-Bus and various sensors. Wired to satellite and cellular antennas. Potentially connects to mobile device/in-cab terminal via Bluetooth (optional).
		Satellite and Cellular Antennas	....
		GPS Satellite Receiver	Receives signals from GPS satellites to pinpoint exact physical location of the vehicle.
		GPS Chip GSM Jamming Detection/Alert	Contains GPS chip that has the capability of detecting a jamming attack. Chip is programmed to detect and alert if a jamming attack is launched against the tractor's telematics system.
		Hybrid satellite/cellular modem	Contains hybrid satellite/cellular modem. Satellite channel rarely used – only when shipment is in a cellular dark zone or if cellular communications are jammed. Refer to Figures IV-3 and IV-4 for location/event reporting.
	Sensors	Impact/Accident Alert (Accelerometer)	Detects sudden impact or rollover – indicative of a crash or attack.
		Equipment Tampering Detection	Detects if equipment is disabled or malfunctioning (inoperable).
		Trailer/Tanker Connect/Disconnect	Detects when a trailer or tanker is connected/disconnected to a tractor. This is particularly an issue between gate-out and gate-in for an unplanned or unscheduled trailer or tanker disconnect or if a trailer or tanker is disconnected at an unknown or unplanned consignee location.
		Ignition State	Provides status of truck engine – on/off

SECURITY EOBR
(TRACTOR-BASED TELEMATICS SYSTEM)

Communications and Messaging (in addition to DOT EOBR)	Event Based Messaging	Gate-Out and Gate-In	Rest-In/Rest-Out (optional)	Ignition On or Off
		Stop Greater Than xx Minutes	Panic Button	Driver Outgoing Call to Tracking Center
		Tracking Center Call Received by Driver	Cross State Boundary	Enter High Threat Urban Area Exit High Threat Urban Area
		Trailer/Tanker Disconnect	Equipment Tampering	GPS/GSM Jamming
		Impact, Accident, or Roll Over	Enter Cellular Dark Zone	Exit Cellular Dark Zone
		Enter No Drive Zone	Disable Signal Received	Enter/Exit Geofenced Areas
	Machine to Machine Security EOBR/tracking center	Tractor Disabling Incoming Message	When a vehicle receives a disabling message from the truck tracking center, the Security EOBR will bring the truck to a stop and trigger the horns/lights of the vehicle.	
		No Drive Zone Signal	No Drive Zones are special geofenced areas established by TSA. Systems at the tracking center will automatically send a message to the Security EOBR when that truck enters a No Drive Zone. The Security EOBR should be capable of accepting the signal and bringing the vehicle to a stop.	
		Variable Location Reporting Incoming Message	The shipment tracking center may automatically or manually send a message to the Security EOBR directing it to report location more (or less) frequently.	
	Other Machine to Machine	Electronic Manifest Transactions	Driver will have smart phone or other mobile device with an electronic manifest application. The application allows the driver and shipper to execute electronic manifest transactions including application of a digital signature at the time that custody of the Tier 1 HSSM materials pass from the shipper to the driver. Digital signatures and other electronic manifest transactions are recorded at shipment tracking center via cellular network.	
		Tractor Identification Transponder	Transponder broadcasts tractor identification.	
		Over the Air Programming	The Security EOBR can accept software updates over the air.	
Physical Hardening		Wires & Antennas	Wiring must be secured to prevent physical disabling.	
		Device Installation/Location	Antennas and other system components must be installed to prevent them from being easily identified and disabled.	
		System Redundancy	TBD	

Figure III-7.

• • •

IV.

TSA's Tier 1 HSSM shipment tracking program should embrace a concept of operations plan that focuses on hazmat supply chain risk reduction.

CONCEPT OF OPERATIONS PLAN
TIER 1 HSSM SHIPMENT TRACKING PROGRAM

The total cost of a Tier 1 HSSM shipment tracking program reflects not only the cost of carrier telematics systems but also other costs such as the cost of regulatory compliance and the cost of operating a shipment tracking center (Public Sector Reporting Center).

This section describes a concept of operations plan for TSA's Tier 1 HSSM shipment tracking program. The concept of operations plan describes how a Public Sector Reporting Center will work in conjunction with tractor- and trailer-based telematics systems detailed in Section III. It also describes the regulatory infrastructure that TSA would likely put in place to implement a Section 1554-compliant shipment tracking program.

This concept of operations plan forms the basis for the project team's estimate of the total cost of a Tier 1 HSSM shipment tracking program (refer to Section V).

What does TSA need in a Public Sector Reporting Center?

FMCSA's 2004 Hazardous Materials Safety and Security Technology Field Operational Test (2004) first advanced the concept of the Public Sector Reporting Center, a centralized tracking/monitoring facility for shipments of hazardous materials. A general concept of operations plan was presented in which the Public Sector Reporting Center would integrate information gathered from telematics systems deployed by hazmat carriers to create a centralized information processing and command/control capability. The study envisioned that enhanced information exchange between public and private sector hazmat stakeholders would provide law enforcement and emergency response personnel access to accurate, timely, and action-oriented information. The FMCSA study projected that the implementation of a Public Sector Reporting Center would generate security benefits exceeding $1 Billion.

Development of a Public Sector Reporting Center concept of operations plan was not the main focus of the FMCSA study, however, and FMCSA recommended a follow-on study to assess the feasibility of implementing a Public Sector Reporting Center for hazmat shipments.

Based on FMCSA's recommendation, Congress directed TSA to conduct its Hazmat Truck Security Pilot (2007) to determine if a Public Sector Reporting Center was feasible. A technology prototype of a hazmat shipment tracking system was built and operated on a limited basis. The study proved that development of a Public Sector Reporting Center was feasible from a technology perspective. However, the technology prototype fell far short of an operational shipment tracking system for Tier 1 HSSMs. Also, the Pilot did not examine many of the technology, cost, and programmatic issues that would be important in implementing a national shipment tracking system for Tier 1 HSSMs.

TSA's Fedtrak R&D initiative picked up where the Hazmat Truck Security Pilot left off with the aim of building the software and systems needed to support an operational Tier 1 HSSM shipment tracking program. The Fedtrak project team conducted a detailed gap analysis of the Hazmat Truck Security Pilot technology prototype and used that gap analysis, in part, to construct an architectural plan for an operational Tier 1 HSSM shipment tracking system. The team also completed an analysis of TSA's future operating requirements, including those related to Section 1554, and constructed a set of requirements for TSA's Public Sector Reporting Center.

A Public Sector Reporting Center is more than just shipment tracking. A common misperception is that shipment tracking is the sole function required of a Public Sector Reporting Center. In fact, as illustrated in **Sidebar 5**, TSA's Tier 1 HSSM Public Sector Reporting Center needs to serve a variety of functions.

The Public Sector Reporting Center has to help TSA drive down risk in the hazmat supply chain. Risk is defined by the U.S. Department of Homeland Security as Risk = Threat x Vulnerability x Consequence. FMCSA's Hazardous Materials Safety and Security Technology Field Operational Test quantified security benefit as a function of the reduction in vulnerability a technology or practice offered. For example, deployment of a certain telematics technology would offer x% reduction in the security vulnerability of a shipment (refer to Section V and Annex D for more detail). Practices that work to reduce shipment

What is a Tier 1 HSSM Public Sector Reporting Center?

- 24/7/365 real-time tracking platform for Tier 1 HSSM shipments that provides TSA visibility into the movement of Tier 1 HSSM shipments over the nation's road system

- risk management platform that identifies the riskiest en-route shipments on a real-time basis and allows TSA to proactively manage risk in the hazmat supply chain

- implementing tool for a TSA Tier 1 HSSM regulatory program focused on supply chain risk reduction

- tool for Tier 1 HSSM shippers, carriers and consignees that have Tier 1 HSSM regulatory compliance responsibilities

- electronic manifest and routing solution for Tier 1 HSSM shipments (chain-of-custody and route adherence monitoring)

- collaboration platform to manage Tier 1 HSSM security incidents by bringing together federal, state, and local response agencies as well as HSSM trading partners (shippers, carriers, and consignees) in the resolution of the incident

- extensive warehouse of data on Tier 1 HSSM transactions/shipments over U.S. roads

SIDEBAR 5.

vulnerability, and by extension supply chain risk, include the following:

- deployment of tractor- and trailer-based telematics systems;

- Public Sector Reporting Center – 24/7/365 shipment tracking/monitoring;

- Public Sector Reporting Center – risk platform;

- enhanced telematics functionality (ex. anti-jamming, vehicle disabling);

- electronic manifest processing – chain of custody control; and

- physical hardening of telematics systems.

A Public Sector Reporting Center will house systems and capabilities that reduce shipment vulnerability and TSA's objective should be to optimize these systems and capabilities to maximize vulnerability reduction.

Real-time shipment tracking is easy, but real-time supply chain risk management is challenging. In the highway mode, a terrorist can take control of a truck – anywhere along its route - and drive it to a target where it and/or its contents can be used as a weapon. Also, as a truck moves over the highways, its risk posture changes. It changes because of what is around the truck and the danger that the truck and its contents pose to what is around it. For example, a truck moving into a high threat urban area carrying a toxic inhalation gas is "riskier" than a truck in a rural area carrying a less lethal material. A Public Sector Reporting Center has to have the systems capability to manage risk on a real-time basis. In TSA's Fedtrak R&D initiative, an approach called "dynamic risk profiling" has been developed in which a risk score for a shipment is generated each time a truck changes locations. A risk engine coupled with a shipment tracking system employs sophisticated geo-based algorithms to calculate risk using DHS's threat, vulnerability, consequence (T,V,C) paradigm for risk. The Fedtrak risk engine generates relative risk scores which allows for the identification of the riskiest shipments on the road at any time. This dynamic risk profiling approach allows the Public Sector Reporting Center to serve as a risk management platform as well as a shipment tracking platform.

A Public Sector Reporting Center has to integrate the business processes of Tier1 HSSM trading partners. A shipment of Tier 1 HSSMs involves three trading partners – shippers, carriers, and consignees. Tier 1 HSSM trading partners are linked by common security objectives and by business processes that dictate the way the trading partners interact. An efficient Public Sector Reporting Center will integrate the business processes of Tier 1 HSSM trading partners. One exceptionally important set of business process that a Public Sector Reporting Center should support are those associated with an electronic manifest system. In a Tier 1 HSSM electronic manifest system, shippers (or carriers) will prepare an electronic manifest – essentially an electronic version of the required DOT shipping paper. Using a hand-held mobile device, a carrier will apply a digital signature to the manifest when the carrier assumes stewardship of the Tier 1 HSSM shipment at the shipper's location. The consignee will apply a digital signature when the consignee takes delivery of the Tier 1 HSSM shipment from the carrier. Electronic manifest programs are increasingly being adopted by Federal agencies. The United States Customs and Border Protection (CBP) requires an electronic manifest for all in-bound shipments of goods by truck from Canada and Mexico. In October 2012, the United States Environmental Protection Agency (EPA) obtained authority to implement an electronic manifest program for hazardous waste shipments. Also in 2012, MAP-21 legislation authorized DOT to implement pilot studies for electronic shipping papers (e.g. electronic manifests). The project team expects that tighter chain-of-custody control resulting from a Tier 1 HSSM electronic manifest program will significantly reduce shipment vulnerability, especially those related to insider threats. Chain-of-custody control for Tier 1 HSSM shipments, the riskiest and most dangerous shipments traveling over the roads, should be at least as tight as EPA's chain-of-custody control for hazardous waste shipments.

A Public Sector Reporting Center has to efficiently integrate the data flowing from tractor- and trailer-based telematics systems. A constant flow of messages will flow from tractor- and trailer-telematics systems to a Public Sector Reporting Center. For example, Section III described the message sets that the Security EOBR will "push" into a Public Sector Reporting Center. An efficient interface with tractor- and trailer-based telematics systems is a critical success factor for a Public Sector Reporting Center. As noted in Section III, this interface has to support the "2-way" flow of messages on a machine-to-machine (M2M) basis. For example, systems at the Public Sector Reporting Center have to be able to "tell" tractor-based telematics systems to increase location reporting when the tractor is in or approaching a TSA High Threat Urban Area.

A Public Sector Reporting Center has to be manned 24/7/365. There are about 2 million Tier 1 HSSM shipments per year in the United States – or over 5,000 shipments per day. The vehicles carrying these shipments are in constant motion, often traveling near or through the nation's metropolitan areas including TSA's 50+ High Threat Urban Areas. While systems are useful in tracking and prioritizing security risks, systems are not a substitute for human oversight/judgment. Tier 1 HSSM shipments travel over the nation's roads 24/7/365 and a Public Sector Reporting Center needs to be staffed accordingly.

The operation of a Public Sector Reporting Center has to respect federal/state/local governmental structures. State and/or local responders will take the response lead in the majority of security incidents – at least initially. TSA's Public Sector Reporting Center has to respect the roles and responsibilities to State and local governments and their on-going informational needs.

Tier 1 HSSM shippers, carriers, and consignees expect a "corporate-grade" web experience. The main customers of a shipment tracking center housed in Public Sector Reporting Center will be corporate trading partners – Tier 1 HSSM shippers, carriers, and consignees. They will expect a "corporate-grade" web experience that employs the latest web technologies as well as top-quality customer service. Thus, a Public Sector Reporting Center not only has to create exceptional tracking systems for its corporate customers, it has to create customer service systems that meet their needs as well. Constant investment to keep systems and services up to date is a critical success factor for a Public Sector Reporting Center.

Security Specialists at the Public Sector Reporting Center need to be able to reach out to drivers to resolve incidents. Security Specialists at the Public Sector Reporting Center need to respond when they suspect a security incident is occurring. For example, a panic button alert will spur a Security Specialist into action. In almost every situation, the Specialist will need to talk with drivers in the investigation and/or resolution of an incident. In Section III, the project team recommended that the Security EOBR incorporate a "push to talk" button on the in-cab terminal (refer to Figures III-6 and III-7) that will allow a driver to directly contact a Security Specialist at the Public Sector Reporting Center. Conversely, systems at the Public Sector Reporting Center need to give the Security Specialist the capability to contact the driver in-cab without using the driver's cell phone.

Regulations have to drive telematics deployment and data reporting to a Public Sector Reporting Center. Section II highlighted the need for regulations to drive the deployment of truck telematics systems. In addition, FMCSA concluded in its Hazardous Materials Safety and Security Technology Field Operational Test that carriers will not report data to a Public Sector Reporting Center without a regulatory driver. TSA's Hazmat Truck Security Pilot reaffirmed this point as well. A Public Sector Reporting Center will, of course, fail if carriers refuse to report data.

How will the Public Sector Reporting Center work?

The Fedtrak project team constructed a high-level architectural plan for a Public Sector Reporting Center as illustrated in **Figure IV-1**.

The architectural plan reflects the requirements analysis completed by the Fedtrak project team, and satisfies the requirements of Section 1554 of the 9/11 Act.

What regulatory infrastructure is needed to support a Tier 1 HSSM shipment tracking program?

In 2004, FMCSA's Hazardous Materials Safety and Security Operational Field Test concluded that hazmat carriers will not deploy truck telematics systems in the absence of a regulatory requirement to do so – even though truck telematics systems generate significant cost savings for carriers. More recently, DOT – and Congress via the MAP-21 legislation - concluded that regulations are needed to drive its EOBR/Hours of Service program. Otherwise, carriers will not widely deploy EOBRs.

A Tier 1 HSSM shipment tracking program is dependent on deployment of telematics systems, and like DOT's EOBR/HOS program, regulations will need to drive telematics deployment. In addition, regulations will provide the infrastructure in which a Tier 1 HSSM shipment tracking program will operate.

The following describes elements of a regulatory program that will support the concept of operations plan described in this section.

TSA will regulate Tier 1 HSSM shipments. TSA will focus its regulatory effort on Tier 1 HSSM shipments, the riskiest materials on the road from a security perspective, and on the activities of those companies engaged in shipping, transporting, and receiving HSSMs (i.e. HSSM shippers, carriers, and consignees).

Tier 1 HSSM shippers, carriers, and consignees will register with the Public Sector Reporting Center, creating a "trusted trading partner" network. Tier 1 HSSM shippers, carriers and consignees will register with the Public Sector Reporting Center. Shippers will register their shipping locations and the HSSMs they will ship from each. Carriers will register their vehicles, telematics devices and drivers. In addition, shippers will initiate a business process that will link shippers, carriers, and consignees in a "trusted trading partner" network. In the trusted trading partner context, a shipper cannot release a Tier 1 HSSM shipment to a carrier unless the shipper and the carrier have a pre-established trading partner relationship.

Tier 1 HSSM carriers will deploy a Security EOBR and trailer/tanker telematics system and report data to a Public Sector Reporting Center. TSA's HSSM rule will be technology forcing, much like DOT's EOBR regulation. Tier 1 HSSM carriers will be required to deploy a Security EOBR that meets TSA-specified performance requirements. Carriers will also report data – in a form and fashion acceptable to TSA – to a Public Sector Reporting Center. Section III describes technology performance requirements for the Security EOBR and data reporting requirements.

An electronic manifest program will provide chain-of-custody control over Tier 1 HSSM shipments and enable dynamic risk profiling. An electronic manifest program enables the Public Sector Reporting Center to serve both as a tracking and a risk management platform. Shippers/carriers will prepare an electronic manifest for each Tier 1 HSSM shipment. The electronic manifest will include all DOT-required shipping paper data elements including type/quantity of materials in the shipment and the identification of the shipper, carrier, and consignee(s). Shippers/carriers will submit the electronic manifest to the Public Sector Reporting Center before the carrier arrives at the shipper's location to take custody of the shipment. The driver will apply a digital signature to the manifest before gate-out using a smart phone application, indicating that the driver has assumed custody of the shipment. The consignee will apply a digital signature to the electronic manifest when the consignee assumes custody of the shipment.

An electronic manifest enables dynamic risk profiling by providing the risk engine data on type/quantity of materials in a shipment. Beyond dynamic risk profiling, an electronic manifest will give TSA chain-of-custody control over Tier 1 HSSM shipments. For example, shippers will not be allowed to release a Tier 1 HSSM shipment to an unauthorized driver/carrier. TSA's electronic manifest regulation will provide chain-of-custody control as least as strong as EPA's upcoming electronic manifest rule for hazardous waste shipments.

An electronic trip/route plan will enable route adherence monitoring. Tier 1 HSSM carriers will also file an electronic route/trip plan with the Public Sector Reporting Center before shipment gate out. The route plan will specify the routes and alternate routes the carrier intends to follow – from the shipping location to the consignees. The Public Sector Reporting Center will track the shipment to ensure that the shipment is following planned routes as expected.

TSA Tier 1 HSSM regulations will incorporate/update existing DOT hazmat regulations, and focus on reducing risk in the hazmat supply chain. DOT requires carriers of certain materials to obtain hazmat safety permits. Essentially this is the same set of materials as TSA's Tier 1 HSSM group. Also, DOT requires shippers and carriers of these materials to prepare and follow hazmat security plans. TSA should leverage existing DOT rules.   This not only promotes regulatory efficiency, but the costs of existing rules have already been absorbed by TSA's regulated community. Ideally, TSA and DOT will pursue a joint safety/security rule for HSSMs – and in the process, update existing rules on the books.

Maximizing security benefit will be TSA's objective. FMCSA's Hazardous Materials Safety & Security Operational Field Test established a methodology to quantify security benefits based on reduction in vulnerability in the risk equation where Risk = Threat x Vulnerability x Consequence. For example, the use of telematics will reduce the vulnerability of a shipment to theft or diversion. The regulatory measures TSA takes should all be designed to directly reduce vulnerability. The following regulatory measures will reduce vulnerability and in doing so, increase security benefits.

Deployment of enhanced telematics systems maximize vulnerability reduction (refer to Section III)

24/7/365 real-time shipment tracking/monitoring at a Public Sector Reporting Center

24/7/365 real-time shipment risk monitoring at a Public Sector Reporting Center

Enhanced telematics functionality such as jamming detection and vehicle disabling

Electronic manifest processing – chain of custody control for en-route shipments

Physical hardening of vehicles and telematics systems

More emphasis on Tier 1 HSSM shippers. Traditionally, DOT has focused much of its regulatory scrutiny on the safety posture/performance of carriers with carriers being primarily responsible for the safety of a shipment. On the other hand, EPA views hazardous waste carriers (transporters) as passive participants in its hazardous waste regulatory program. Instead, shippers are responsible for hazardous waste from "cradle to grave". In its security program, TSA should fall somewhere in between, especially in its adoption of an electronic manifest regulatory mechanism. From a regulatory philosophy point of view, TSA should consider adopting the following hybrid view.

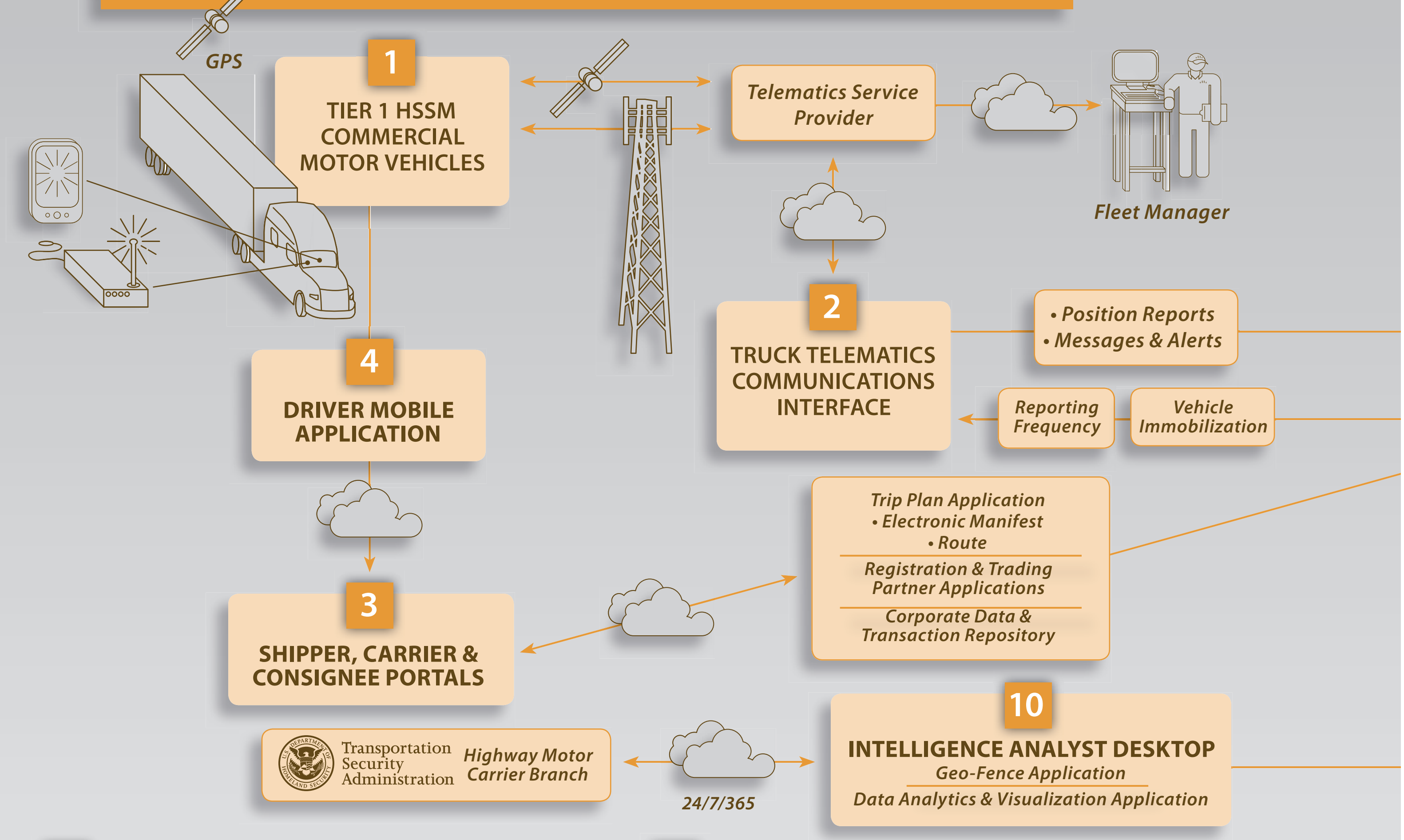
Shippers are responsible for overseeing chain-of-custody control over a shipment – all the way from the shipper's location to the consignee.

Shippers are responsible for contracting with carriers that are security and safety capable.

Carriers are responsible for following procedures to ensure en-route shipment security and safety.

The Transported Asset Protection Association (TAPA) is an industry group that has set up certification programs to support companies that ship and transport high value goods. Under TAPA programs, shippers select carriers that have achieved certification (from independent auditors) for their trucking security programs. Beyond being a model for the relationship that TSA might promote between HSSM shippers and carriers, a TSA regulatory program that recognizes (or requires) carrier certification could be an excellent way for TSA to leverage scarce inspection and enforcement resources.

Figure IV-1. Public Sector Reporting Center Architectural Schematic (Fedtrak R&D)


GPS
1
TIER 1 HSSM COMMERCIAL MOTOR VEHICLES
Telematics Service Provider
Fleet Manager
2
TRUCK TELEMATICS COMMUNICATIONS INTERFACE
• Position Reports
• Messages & Alerts
Reporting Frequency
Vehicle Immobilization
4
DRIVER MOBILE APPLICATION
Trip Plan Application
• Electronic Manifest
• Route
Registration & Trading Partner Applications
Corporate Data & Transaction Repository
3
SHIPPER, CARRIER & CONSIGNEE PORTALS
Transportation Security Administration
Highway Motor Carrier Branch
24/7/365
10
INTELLIGENCE ANALYST DESKTOP
Geo-Fence Application
Data Analytics & Visualization Application

1 **TRACTOR- AND TRAILER-BASED TELEMATICS.** Tier 1 HSSM carriers will deploy truck and trailer-based telematics systems, and data from those systems will travel over cellular or satellite systems to commercial telematics service providers. Section III describes the telematics systems the project team recommends that Tier 1 HSSM carriers deploy. The telematics service providers will provide aggregated fleet information to carrier fleet managers. Normally, the fleet manager will also purchase software services from a telematics service provider to support full fleet oversight, shipment routing, dispatch logistics, driver behavior monitoring, etc.

2 **INTERFACE WITH PUBLIC SECTOR REPORTING CENTER.** A portion of the data stream flowing from truck and trailer-based telematics systems – truck identification/location and various message sets – will be parsed out by the telematics service provider and sent to the Public Sector Reporting Center via an interface. TSA regulations will dictate the form, fashion and frequency of data/message reporting to the Public Sector Reporting Center (refer to Section III).

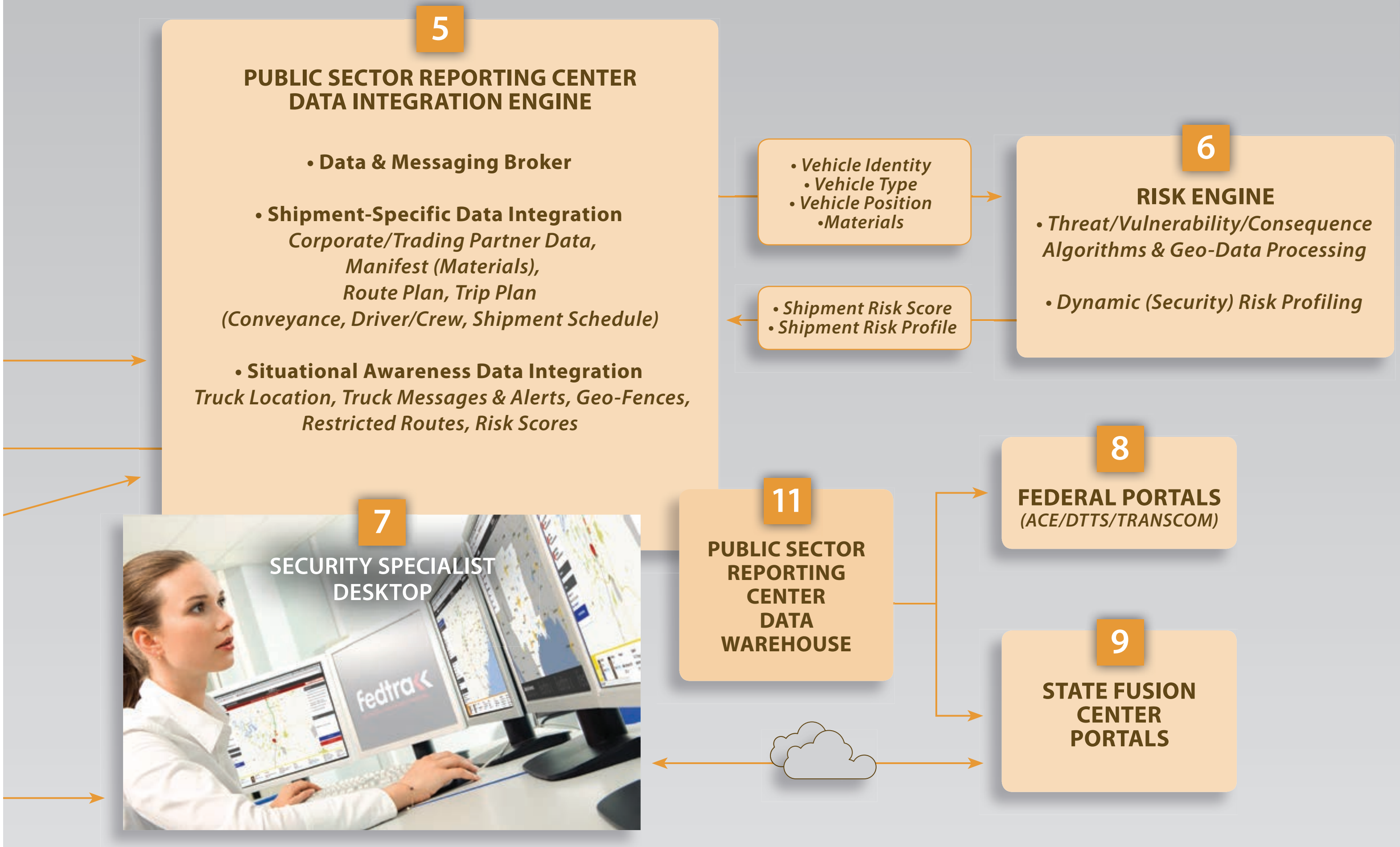
3 **SHIPPER, CARRIER, AND CONSIGNEE PORTALS.** Information on shipment type and quantity and route will be provided to the Public Sector Reporting Center by shippers and carriers via portals. Electronic manifests provide information on type and quantity of HSSMs in a shipment and other important shipment information. The trip/route plan provides the Public Sector Reporting Center with information on drivers, conveyance and route. TSA regulations will require electronic manifest and trip/route plan submission before shipment gate-out.

4 **DRIVER MOBILE APPLICATION (ELECTRONIC MANIFEST).** The driver will be equipped with a smart phone and a Public Sector Reporting Center application that will allow the driver to complete electronic manifest applications in the field, including digital signatures. The mobile application will allow a driver to:

- make final edits to an electronic manifest such as quantity/type of HSSM in the shipment while at the shipper location and apply digital signature to electronic manifest;
- send geo-coded panic alerts to the Public Sector Reporting Center; and
- signal gate-out at shipper facility and signal gate-in at consignee facility.

5 **DATA INTEGRATION ENGINE – PUBLIC SECTOR REPORTING CENTER.** The Public Sector Reporting Center's Data Integration Engine will continually mash together information from vehicle telematics systems with electronic manifests and trip/route plans to create actionable intelligence. For example, the following questions about an individual shipment can be answered once the data is processed by the Data Integration Engine.

- What is the truck carrying? What is the shipment risk profile?
- Who is driving the truck? What is the truck's location?



5

PUBLIC SECTOR REPORTING CENTER DATA INTEGRATION ENGINE

- Data & Messaging Broker
- Shipment-Specific Data Integration *Corporate/Trading Partner Data, Manifest (Materials), Route Plan, Trip Plan (Conveyance, Driver/Crew, Shipment Schedule)*
- Situational Awareness Data Integration *Truck Location, Truck Messages & Alerts, Geo-Fences, Restricted Routes, Risk Scores*

• Vehicle Identity
• Vehicle Type
• Vehicle Position
•Materials

• Shipment Risk Score
• Shipment Risk Profile

6

RISK ENGINE

- *Threat/Vulnerability/Consequence Algorithms & Geo-Data Processing*
- *Dynamic (Security) Risk Profiling*

7

SECURITY SPECIALIST DESKTOP

11

PUBLIC SECTOR REPORTING CENTER DATA WAREHOUSE

8

FEDERAL PORTALS
(ACE/DTTS/TRANSCOM)

9

STATE FUSION CENTER PORTALS

- What is the truck's destination? Who are the trading partners?
- What route has the truck followed? Is the truck off-route? Off schedule?

The Data Integration Engine will also serve data up to shipper, carrier, and consignee portals.

6 **RISK ENGINE.** The Public Sector Reporting Center Risk Engine is tightly integrated with the Data Integration Engine, and will support dynamic risk profiling of each en-route shipment. TSA's highway program has a unique security challenge. The Risk Engine employs sophisticated geo-based algorithms to calculate risk using DHS's threat, vulnerability, consequence (T,V,C) paradigm for risk. The Risk Engine generates relative risk scores which allows for the identification of the riskiest shipments on the road at any time. The Risk Engine allows the Public Sector Reporting Center to serve as a risk management platform as well as a shipment tracking platform.

7 **SECURITY SPECIALIST DESKTOP.** Integrated data is presented on the Security Specialist Desktop in the Public Sector Reporting Center. The Public Sector Reporting Center will be manned 24/7/365, primarily by Security Specialists, each of whom will be assigned a geographic area to monitor. The Security Specialist Desktop will be a state-of-the-art GIS-based display that provides a Security Specialist the ability to monitor en-route shipments and to support the resolution of security incidents as they occur. The Risk Engine will provide Security Specialists with lists of the riskiest shipments at any time so that those shipments can be closely monitored.

8 **STATE FUSION CENTER PORTALS.** The Public Sector Reporting Center will connect with State fusion centers, the natural federal/state connect point, and will push a continual stream of information to each state fusion center. Data will flow continuously from the Public Sector Reporting Center Data Warehouse to a State Fusion Center Portal. This continuous stream of data will provide the fusion center with the common operating picture of active en-route HSSM shipments that are in the state's boundaries or are in-bound to the state.

9 **FEDERAL PORTALS.** The Public Sector Reporting Center will also exchange information with other Federal systems such as CBP's ACE Truck E-Manifest System, DoD's Defense Transportation Tracking System (DTTS), and DOE's TRANSCOM system.

10 **INTELLIGENCE ANALYST DESKTOP.** The Intelligence Analyst Desktop is intended to be the entry point for intelligence data into the Public Sector Reporting Center. The Intelligence Analyst will evaluate information, and create a list of shipments that needs to be monitored closely by Security Specialists.

11 **PUBLIC SECTOR REPORTING CENTER DATA WAREHOUSE.** Every Tier 1 HSSM shipment will generate considerable data. This data will be stored in the Data Warehouse. As data holdings within the Data Warehouse build, the Intelligence Analyst will have the ability to analyze historical data using various geospatial analytical tools and business intelligence tools.

V.

The security benefits of a Tier 1 HSSM shipment tracking program far outweigh the costs of that program.

BENEFIT/COST ANALYSIS
TIER 1 HSSM SHIPMENT TRACKING PROGRAM

Benefits — Tier 1 HSSM Shipment Tracking Program

FMCSA's Hazardous Materials Safety and Security Operational Field Test was a seminal study into the use of truck telematics technology to enhance hazmat shipment safety and security. It was the first and only large-scale test of truck telematics technology, and is particularly notable because the FMCSA project team quantified the costs and benefits associated with telematics technology deployment by hazmat carriers.

Three types of benefits were evaluated in FMCSA's Hazardous Materials Safety & Security Operational Field Test: efficiency benefits, safety benefits, and security benefits.

Truck telematics systems save carriers money by making their operations more efficient – routing is more efficient, scheduling is more efficient, and less fuel is consumed. Many large, long-haul carriers have already installed truck telematics systems offered from telematics service providers such as Qualcomm and PeopleNet. FMCSA's Hazardous Materials Safety & Security Operational Field Test (FOT) estimated the unit cost operational efficiency benefits associated with the deployment and use of truck telematics systems.[1] As illustrated in **Figure V-1**, the FOT estimated that a typical bulk chemicals carrier would save $7,116/truck/year after deploying a basic truck telematics system. An explosives carrier would save $10,968/truck/year.[2] Most bulk chemicals and explosives are Tier 1 Highway Security Sensitive Materials.

TELEMATICS AND OPERATIONAL BENEFITS

Operational Benefits	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	$253/month a. $19 b. $122 c. $37 d. $65 e. $11	$491/month a. $30 b. $81 c. $290 d. $78 e. $13
Improved Maintenance Scheduling • Reduces maintenance & repair cost • Increases revenue miles by reducing downtime	$18/month	$37/month
Reduce Out-Of-Route Mile • Creates savings of line haul variable costs	$123/month	$116/month
Improved Vehicle Utilization by Reducing Empty Miles • Increases potential number of trips	$199/month	$270/month
Total Monthly Benefit Per Truck	$593/month	$914/month
Total Annual Benefit Per Truck	**$7,116/year**	**$10,968/year**

Figure V-1.

The operational efficiency benefits arising from truck telematics systems far exceed the cost of deploying and operating truck telematics systems. Cost savings due to efficiency gains is, in fact, the key value proposition offered by telematics service providers to fleet managers.

Operational efficiency benefits cannot be included in a benefits/cost analysis in a TSA security rule, however, and were not included in the benefit/cost analysis completed in this project. This reflects the precedent set in DOT's Electronic On Board Recorder/Hours of Service (EOBR/HOS) regulatory initiative. In its Regulatory Impact Analysis for the EOBR/HOS regulation, DOT did not include operational efficiency benefits in its benefit/cost analysis even though the EOBR, a basic telematics device, allows carriers to capture efficiency benefits in addition to safety benefits. DOT's HOS rule had to stand solely on the safety benefits generated by deployment of EOBRs on commercial vehicles and could not include other types of benefits such as operational efficiency benefits.

TSA's situation is similar. Although a carrier might capture significant efficiency and safety benefits by deploying a telematics system to meet a TSA regulatory requirement, a security-based telematics rule offered by TSA must rest solely on the security benefits offered by the deployment of the telematics system.

The FOT quantified security benefits associated with the deployment of truck telematics systems and the implementation of a shipment tracking center.[3] A detailed

[1] FMCSA Hazmat Safety and Security Technology Field Operational Test http://www.fmcsa.dot.gov/safety-security/hazmat/fot/index.htm

[2] Table 5-2, page 43 FMCSA Hazmat Safety and Security Technology Field Operational Test

[3] FMCSA Hazmat Safety and Security Technology Field Operational Test http://www.fmcsa.dot.gov/safety-security/hazmat/fot/eval-rpt-synthesis-intro.htm - pages 47-60

and comprehensive methodology was used to quantify security benefits. Essentially, a panel of subject matter experts determined vulnerability reduction that would be captured by deploying various combinations of telematics equipment on trucks. Security benefit was calculated by multiplying vulnerability reduction by reasonable worse case consequences.

A detailed discussion of the security benefits methodology from FMCSA's Hazmat Safety and Security Technology Field Operational Test may be found in **Annex C.**

The FOT project team reached the clear conclusion that deployment of truck telematics systems will generate immense security benefits. **For Tier 1 HSSM shipments, the security benefit will exceed $5 Billion** – ranging from $3.5 Billion for explosives shipments and $5.3 Billion for bulk chemical shipments.

Figure V-2 summarizes security benefits that would be captured if Tier 1 HSSM carriers (bulk chemicals, explosives) deployed truck telematics systems. The last two telematics packages in the table (highlighted text) are closest to the telematics portfolio that TSA might need for its highway hazmat security program.

The FOT was completed in 2004. However, the security benefits findings from the study are still valid and relevant to the Section 1554 benefit/cost analysis.

The security benefits methodology in FOT was sophisticated, comprehensive, and consistent with current DHS risk approaches. The FMCSA project team employed a sophisticated and comprehensive approach to quantifying benefits, especially security benefits. The methodology was based on the 'threat, vulnerability, consequence' risk approach in use today at DHS as well as specific threat scenarios that TSA has incorporated into its highway program. A large group of subject matter experts from industry and government fed their expertise into the FOT.

Explosives and bulk chemicals are Tier 1 HSSMs. The FOT was completed before TSA issued its list of Tier 1 HSSMs – the riskiest materials on the nation's roads. However, two groups of hazardous materials studied – explosives and bulk chemicals – are Tier 1 HSSMs. As "pure play" Tier 1 HSSMs, conclusions reached by the FMCSA project team in terms of benefits for these materials are applicable to TSA's present day highway hazmat security program.

Security benefits are likely understated. The FOT quantified security benefits using the standard DOT/DHS risk equation in which Risk (cost) = Threat x Vulnerability x Consequence. In general, the security benefit is a function of the amount of vulnerability reduction that telematics systems offer for explosives shipments or bulk chemical shipments. Vulnerability reduction in the study is likely understated – perhaps significantly so – in relation the vulnerability reduction that TSA might capture with an enhanced "security" telematics package, tighter chain-of-custody control via an electronic manifest program, and closer shipment monitoring via centralized shipment tracking.

The FOT also touched on an important issue related to security benefits and carrier behavior. The study concluded that carriers will not widely deploy truck telematics equipment, even if there is a clear and compelling benefit to the carriers, in the absence of a regulatory requirement to do so.

> *"… 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 study also concluded that the security benefits offered by telematics would be lost if the technology was not fully deployed.

> *"It should be noted that partial deployment might not nec-*

TRUCK TELEMATICS AND SECURITY BENEFITS – TIER 1 HSSM SHIPMENTS

	Vulnerability Reduction %		Security Benefit (in Millions of Dollars)	
Telematics Technology Package	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives
WC + GPS Position	16%	12%	$2,581	$1,657
WC + GPS Position + Panic Alert	25%	21%	$4,058	$2,822
WC + GPS Position + PSRC	24%	20%	$3,891	$2,652
WC + GPS Position + Vehicle Disabling + Panic Alert	31%	**25%**	**$5,098**	$3,355
WC + GPS Position + Panic Alert + Driver ID + ESCM	33%	**26%**	**$5,319**	**$3,510**

Figure V-2.

essarily result in a directly proportional security benefit. In other words, 50 percent deployment may not yield 50 percent of achievable security benefits. This may occur because while the technology-equipped fleet may not be attacked, a non-equipped fleet would possibly be targeted instead. The deterrent effect of the technologies, if partly deployed, could simply shift terrorist targeting from one fleet to another, with no net change in overall security. Under this assumption, then full deployment is required to realize the security benefits."

Costs — Tier 1 HSSM Shipment Tracking Program

In Section IV, the project team described a Concept of Operations plan for TSA's Tier 1 HSSM truck tracking program that includes the implementation of a regulatory program that will require Tier 1 HSSM carriers to deploy telematics systems and report data to a shipment tracking center. The objective of Section IV was to describe how TSA's overall Tier 1 HSSM tracking program might work so that the costs of the program could be estimated and compared to the security benefits that the program would generate.

The project team summarized Tier 1 HSSM program costs into three categories: 1) telematics capital and operating costs; 2) compliance costs; and 3) centralized shipment tracking costs. In compiling costs, the project team needed to answer the following questions.

How many Tier 1 HSSM shipments are there per year?

What is the unit capital cost for tractor- and trailer-based telematics systems?

What is the annual operating cost of tractor- and trailer- based telematics systems?

How many tractors or straight trucks need to be equipped with telematics equipment?
How many trailers need to be equipped with telematics equipment?

What is the compliance cost of a Tier 1 HSSM regulatory program?

What is the cost of establishing and operating a shipment tracking center?

The project team estimates that there are about 2 million Tier 1 HSSM shipments per year in the United States. About 5,000 tractors, 1,750 straight trucks and 10,625 trailers/tankers will be used for Tier 1 HSSM shipments.

The project team's detailed cost findings are summarized in **Annex D** including a projection of Tier 1 HSSM program costs over time.

Benefit/Cost — Tier 1 HSSM Shipment Tracking Program

A regulatory program that requires Tier 1 HSSM carriers to deploy truck telematics systems and report data to a truck tracking center will significantly reduce risk in the hazmat supply chain. The value of this reduced risk (security benefit) exceeds $5 Billion.

In FMCSA's Hazardous Materials Safety & Security Operational Field Test (FOY), the FOT project team compared benefits and costs using benefit/cost ratios and breakeven analyses. The FOT project team explained its breakeven analysis as follows.

> "… the security benefits were derived under the assumption that threat is held constant at a 100 percent chance that an attempt will be made over the next 3 years on/using a hazmat load for a terrorist attack. Realizing that threat can be unpredictable and vary over time, breakeven numbers of successful attacks that would need to be reduced via the technologies to equal the costs of deploying the technologies is proffered. These breakeven values were calculated using the following formula: **Breakeven Number of Attacks = (Total Deployment Cost for the Technology / Consequence per Attack).**[4]
>
> The breakeven probabilities are presented as a decision tool – if one believes that the probability of an attack (threat) is greater than the breakeven for a technology combination for a load type, so then to society, the investment in the technology combination can be considered sound."

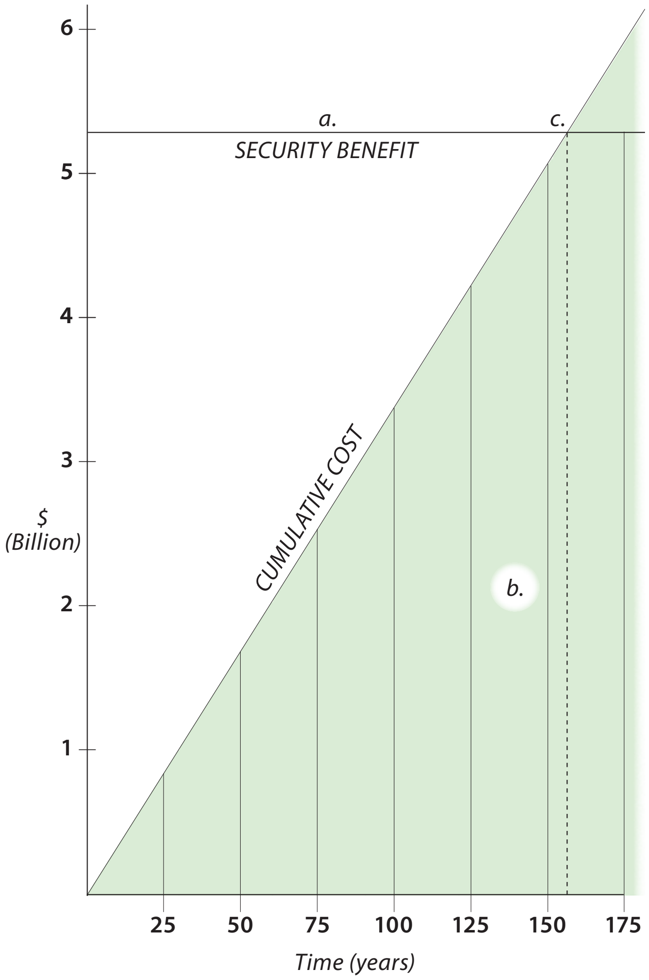
For the Section 1554 evaluation, the Section 1554 project team used both a 3-year and a 10-year timeframe to compare benefits and costs. Figure E-8 in Annex E projects the cost of TSA's Tier 1 HSSM program over time. At 3 years, accumulated costs will total $116,055,250. At 10 years, accumulated costs will total $345,645,750. The benefit/cost ratio of a Tier 1 HSSM truck tracking program will range from 15:1 up to 46:1 based on a comparison of security benefits with accumulated costs as illustrated in **Figure V-3.** Using the breakeven approach from the FOT generates figures for the breakeven number of attacks that could

[4] FMCSA's Hazardous Materials Safety & Security Operational Field Test estimated the Reasonable Worst Cast Per Attack Consequence for bulk chemicals ($16.3 Billion) and truckload explosives (($13.3 Billion). Volume II: Evaluation Final Report Synthesis.

occur in three years or in ten years to warrant investment in a Tier 1 HSSM truck tracking program as illustrated in **Figure V-4**. It is, however, difficult for a policy consumer to use fractional breakeven results in a policy discussion as presented in Figure V-4. For example, knowing that the cost of a Tier 1 HSSM program is justified if .0212 attacks are prevented over the next ten years is too difficult to apply in a policy context. Also, it only gives the policy executive a view of benefits and costs over a set band of time.

A key issue in any breakeven analysis is the time period over which to compare benefits and costs. The FOT project team chose three years as a reasonable amount of time in which a terrorist attack involving a hazmat shipment might occur. However, FMCSA acknowledged that it is not possible to assign probability to a terrorist threat. FMCSA could have easily assumed a longer or even shorter time period as a reasonable time in which a terrorist attack might occur. Also, FMCSA could have assumed multiple attacks might occur in a given time period.

The Section 1554 project team used another approach to conducting a breakeven analysis in addition to the approach adopted by FMCSA in the FOT. The team projected costs into future years to find the point in time at which security benefits are fully absorbed by cumulative program costs. Figure D-8 in Annex D presents the results of this analysis. Assuming security benefits of $5.3 Billion, it will take 157 years for the costs of a Tier 1 HSSM program to fully absorb the benefits as illustrated in **Figure V-5**. This means that if **one terrorist incident** is prevented in the next 157 years by implementing a Tier 1 HSSM tracking program, the cost of that program would be justified.



a. The security benefit of implementing a Tier 1 HSSM shipment tracking program is $5.3 Billion (FMCSA Hazardous Materials Safety & Security Operational Field Test – 2004).

b. The shaded area under the cost line represents the cumulative cost of implementing a Tier 1 HSSM shipment tracking program.

c. At t=157 years, the cumulative cost of implementing a Tier 1 HSSM truck tracking program is equal to the security benefit of that program.

Figure V-5. Benefit/cost breakeven point for implementing a Tier 1 HSSM truck tracking program

BENEFIT/COST RATIO TIER 1 HSSM TRUCK TRACKING PROGRAM				
Security Benefits	Program Costs Time Period – 3 Years	Benefit/Cost Time Period – 3 Years	Program Costs Time Period – 10 Years	Benefit/Cost Time Period – 10 Years
$5.3 Billion	$116,055,250	46:1	$345,645,750	15:1

Figure V-3.

BREAKEVEN NUMBER OF ATTACKS TIER 1 HSSM TRUCK TRACKING PROGRAM				
Consequence per Attack	Program Costs Time Period – 3 Years	Breakeven Number of Attacks – 3 Years	Program Costs Time Period – 10 Years	Breakeven Number of Attacks – 10 Years
$16.3 Billion	$116,055,250	.0071	$345,645,750	.0212

Figure V-4.

Benefit/cost analyses support a strongly compelling argument that TSA should move forward with a Tier 1 HSSM regulatory program that requires Tier 1 HSSM carriers to deploy truck telematics systems and report data to a shipment tracking center. The following summarize the project team's benefit/cost findings.

1. A Tier 1 HSSM shipment tracking program will generate security benefits of more than $5 Billion. Costs, in relation to benefits, are much lower.

2. Security benefits will outweigh costs by 46:1 using FMCSA's 3-year timeframe for evaluating benefits and costs, or by 15:1 using a more conservative 10-year timeframe. Normally, a benefit/cost ratio greater than 1:1 is sufficient justification for a Federal agency to move forward with a regulatory program.

3. Breakeven analysis shows that if a single terrorist attack involving a Tier 1 HSSM shipment is prevented in the next **157 years**, the cost of a Tier 1 HSSM shipment tracking program is warranted.

• • •

VI.

TSA should implement a Tier 1 HSSM shipment tracking program that requires deployment of tractor and trailer telematics systems and data reporting to a Public Sector Reporting Center.

SUMMARY RECOMMENDATIONS
TIER 1 HSSM SHIPMENT TRACKING PROGRAM

1 IN DEVELOPING A TRACKING PROGRAM FOR SECURITY-SENSITIVE MATERIALS AS CALLED FOR UNDER SECTION 1554 OF THE 9/11 ACT, TSA SHOULD IMPLEMENT A REGULATORY PROGRAM THAT REQUIRES TIER 1 HIGHWAY SECURITY SENSITIVE MATERIALS (HSSM) CARRIERS TO DEPLOY TELEMATICS SYSTEMS AND REPORT DATA TO A PUBLIC SECTOR REPORTING CENTER.

A regulatory program that requires Tier 1 HSSM carriers to deploy truck telematics systems and report data to a shipment tracking center will significantly reduce risk in the hazmat supply chain. The security benefit of this reduced risk is estimated to be at $5.3 billion for Tier 1 shipments according to FMCSA's Hazardous Materials Safety & Security Operational Field Test.

Benefit/cost analyses support a strongly compelling argument that TSA should move forward with a Tier 1 HSSM regulatory program. A breakeven analysis of security benefits and costs indicate that a Tier 1 HSSM truck tracking program is warranted if it prevents a single terrorist attack in the next 157 years. Security benefits outweigh costs by 46:1 using the 3-year timeframe for evaluating benefits and costs adopted in FMCSA's Hazardous Materials Safety & Security Operational Field Test. Security benefits outweigh costs by 15:1 using a more conservative 10-year timeframe. Normally, a benefit/cost ratio greater than 1:1 is sufficient justification for a Federal agency to move forward with a regulatory program.

DOT's recent experience with its Electronic On Board Recorder/Hours of Service initiative argues strongly for a regulatory program to promote technology deployment by Tier 1 HSSM carriers and data reporting by shippers, carriers and consignees, both desirable and necessary measures to capture hazmat supply chain security benefits. DOT found that many commercial motor carriers will not deploy truck-based telematics systems unless regulations require them to do so, even if telematics deployment generates substantial cost savings for carriers as numerous public and private studies have shown. Also, DOT's experience proves that telematics service providers will not invest internal research and development funds to refine their products and services to meet a government requirement unless that requirement is rooted in a regulation that provides the telematics service providers certainty over market size and functionality requirements.

2 TSA AND DOT SHOULD PURSUE A COORDINATED SECURITY/SAFETY RULE FOR HIGHWAY SECURITY SENSITIVE MATERIALS. TSA REGULATIONS SHOULD FOCUS ON SECURITY RISK REDUCTION IN THE HAZMAT SUPPLY CHAIN.

For many years, DOT had sole Federal responsibility for the shipment of hazardous materials over the nation's highways. Two months after 9/11, under the Aviation and Transportation Security Act, TSA was created and placed in DOT. TSA was given broad responsibility and authority for ``security in all modes of transportation'' (49 U.S.C. 114(d)). On March 9, 2003 TSA was moved from DOT to the Department of Homeland Security. With this move, Congress split responsibility for the Federal hazmat mission - with DOT retaining responsibility for hazmat safety and DHS/TSA assuming responsibility for hazmat security.

Since 2002, the Federal government has been building toward a hazmat regulatory program that will require telematics system deployment by high risk hazmat carriers and implementation of a Public Sector Reporting Center. On July 16, 2002, DOT published an Advanced Notice of Proposed Rulemaking (ANPRN) that sought comments on a regulation that would enhance hazmat supply chain security via truck telematics systems and vehicle tracking. On March 25, 2003 DOT issued a final rule requiring high risk hazmat shippers and carriers to prepare and follow a written security plan including security measures for en-route shipments. And on June 30, 2004, DOT issued a rule requiring high risk hazmat carriers to obtain a hazmat safety permit that includes measures for driver/carrier communications.

DOT and TSA have also completed a series of Congressionally-mandated studies intended to lay the foundation for a hazmat security regulatory program including FMCSA's Hazmat Safety and Security Technology Operational Field Test (2004), FMCSA's Untethered Trailer Tracking Report (2005), FMCSA's Vehicle Immobilization Technologies, and TSA's Hazmat Truck Security Pilot (2007).

On December 17, 2003, Homeland Security Presidential Directive No. 7 reiterated TSA's authority over security in all transportation modes and directed DOT and DHS to "collaborate in regulating the transportation of hazardous materials in all modes." On September 28, 2004, DOT and DHS signed a Memorandum of Understanding (MOU) on Roles and Responsibilities. The purpose of the MOU was to facilitate the development and deployment of transportation security measures that promote safety, security, and efficiency in the movement of people and goods.

Collaboration between TSA and DOT is critical as it is impossible to fully separate the hazmat safety and security missions. In fact, they are dependent and mutually reinforcing. Strengthening safety measures for high risk hazmat shipments reinforces the security of those shipments. Conversely, strengthening security measures tends to reinforce shipment safety. For example, introduction of electronic shipping papers to improve hazard communications for first responders will also provide chain-of-custody control for shipments of high risk hazardous materials, a significant boost to shipment security (see §33005 MAP-21 authorizing electronic shipping paper pilot studies).

TSA should collaborate with DOT as TSA implements its Tier 1 HSSM regulatory program. In fact, Section 1554 of the 9/11 Act specifically directs the Administrator to develop its tracking program in consultation with DOT. Ideally, TSA and DOT would collaborate in drafting an integrated safety and security regulation for Tier 1 Highway Security Sensitive Materials (HSSMs). Supply chain risk reduction is a critical success factor for TSA's highway hazmat security program, and TSA's regulatory focus in a combined rule should be on shipment vulnerability reduction, the variable in the risk equation that TSA can most readily influence by a technology and performance-based regulation.[1] Regulatory provisions that reduce shipment vulnerability should be incorporated into TSA's HSSM security rule, including the following:

- a requirement that Tier 1 HSSM carriers deploy a telematics package with enhanced security functionality that lessens a shipment's vulnerability to theft, diversion or interception;

- an electronic manifest program to support Tier 1 HSSM shipment chain-of-custody control and to lessen a shipment's vulnerability to insider threats and shipment diversion;

- data reporting to a central tracking center and 24/7/365 monitoring of all en-route Tier 1 HSSM shipments at the tracking center - with particular focus on the "riskiest of the risky" shipments; and

- establishment of "trusted trading partner" relationships between HSSM shippers, carriers, and consignees that serve to address insider threats in the supply chain and speedier, more productive collaboration during a security incident.

There is significant programmatic benefit to TSA in establishing a collaborative relationship with DOT. DOT has advanced its hazmat safety program far beyond where TSA stands with the hazmat security program, and TSA can use a close working relationship with DOT to bring its hazmat security program into equilibrium with DOT's hazmat safety program. Also, Section 1554 specifically requires TSA to develop its shipment tracking program in consultation with DOT.

3 TSA SHOULD REQUIRE TIER 1 HSSM CARRIERS TO ADOPT A TELEMATICS PACKAGE THAT ADDRESSES SECURITY THREATS IN THE SUPPLY CHAIN AND IS BUILT ON THE FOUNDATION OF DOT'S ELECTRONIC ON BOARD RECORDER.

As part of its Hours of Service initiative, DOT will require almost all commercial motor vehicles to deploy an Electronic On Board Recorder (EOBR) by mid-2015. DOT's

[1] The classic risk equation used by DHS and DOT is: Risk = Threat x Vulnerability x Consequence. Threat is the relative attractiveness of a shipment, vulnerability is the likelihood of a successful attack, and consequence is the magnitude of a successful attack. In FMCSA's Hazmat Safety and Security Technology Operational Field Test, a panel of subject matter experts concluded that the appropriate approach was to view threat – the probability that a given attack scenario may be attempted – as constant. Subject matter experts then determined the vulnerability reduction that would likely be captured by deploying various combinations of telematics equipment on trucks. Security benefit was calculated by multiplying vulnerability reduction by reasonable worse case consequences arising from incidents involving different material types.

EOBR rule, as mandated under the MAP-21 legislation, will require carriers to install basic telematics devices on their trucks that meet minimum functional requirements, including the ability to integrate with a tractor's engine/sensor network, to identify the vehicle's driver, and to report out vehicle location. While the telematics functionality in DOT's EOBR will not fully meet TSA's needs, JBUS integration and GPS/location reporting are both core functions that TSA needs in a telematics security solution.

The project team recommends that TSA leverage DOT's EOBR initiative by enhancing the basic telematics functionality in DOT's EOBR so that it can operate as a combined safety and security EOBR for deployment by Tier 1 HSSM carriers. This **Security EOBR** would not only have the functionality to meet DOT's Hours of Service needs, but would include extra functionality to meet TSA's security needs.

The project team approached its analysis of TSA's telematics needs by beginning with DOT EOBR telematics functionality as a baseline, and then determining what incremental functionality would be needed for TSA's highway hazmat program. Specific threat scenarios facing the highway hazmat security program were evaluated in terms of telematics functionality requirements, and the project team examined telematics systems used in other countries in terms of their security functionality, especially functionality related to the threat of hijacking. The project team also evaluated the event/messaging requirements that would be needed in TSA's security program versus those that support DOT's safety program. The end result was development of the functionality requirements for the Security EOBR.

Given the relatively small market size for the Security EOBR in relation to the DOT EOBR, U.S. telematics service providers may be reluctant to invest R&D funds into refining their current EOBR product/service offerings to meet TSA security needs, at least until TSA issues Tier 1 HSSM regulations. The project team recommends that TSA invest Federal R&D funds into the development and testing of a proof-of-concept Security EOBR. Development and testing of a Security EOBR prototype will help TSA as it adopts specific technology standards in a Tier 1 HSSM rule and will help telematics service providers by easing their R&D burden as they refine their EOBR platforms to meet TSA's security needs.

4 TSA SHOULD ADOPT SHIPMENT TRACKING, SUPPLY CHAIN RISK MANAGEMENT, AND SHIPMENT CHAIN-OF-CUSTODY CONTROL AS ESSENTIAL FEATURES OF A TIER 1 HSSM TRUCK TRACKING SYSTEM.

The FMCSA advanced the concept of the Public Sector Reporting Center (PSRC), a centralized shipment tracking/monitoring facility, in the Congressionally-mandated Hazardous Material Safety and Security Operational Field Test (2004) and found that shipment tracking would enhance hazmat supply chain security. In fact, the FMCSA study indicated that shipment tracking will generate about $1 Billion in security benefits.

Development of a concept of operations plan for a shipment tracking center was not the main focus of the FMCSA study, however, and FMCSA recommended that a follow-on study further assess the viability of the concept from a technology perspective. Acting on the FMCSA recommendation, Congress directed TSA to assess the feasibility of centralized shipment tracking via TSA's Hazmat Truck Security Pilot (HTSP).

TSA's Hazmat Truck Security Pilot proved that a centralized truck tracking system – connected to truck-based telematics devices – was feasible. The technology prototype produced in the pilot fell far short of an operational system, however, and TSA's Fedtrak research & development (R&D) initiative picked up where the Hazmat Truck Security Pilot left off with the aim of building the software and systems needed to support an operational truck tracking center.

A key research objective of the Fedtrak R&D initiative is to embed risk management functionality into TSA's shipment tracking system. The need for this risk management functionality reflects a fundamental security threat facing TSA's highway hazmat security program. In the highway mode, a terrorist can take control of a truck and drive it to a target where it and/or its contents can be used as a weapon. Also, as a truck moves over the highways, its risk profile changes. It changes because of what is around the truck and the danger that truck and its contents pose to what is around it. For example, a truck moving into a high threat urban area carrying a toxic inhalation gas is "riskier" than a truck in a rural area carrying a less lethal material. An approach for the "dynamic risk profiling" of Tier 1 HSSM shipments has been developed in the Fedtrak R&D initiative in which a risk score for a truck is generated each time the truck changes locations. Integrating dynamic risk profiling into the overall shipment tracking system allows the system to serve as a real-time risk management platform as well as a real-time tracking system.

The project team recommends that TSA implement an electronic manifest program for shipments of Tier 1 HSSMs as part of its overall shipment tracking program. Electronic manifest programs are increasingly being adopted by Federal agencies. The United States Customs and Border Protection (CBP) requires an electronic manifest for all in-bound shipments of goods by truck from Canada and Mexico. In October 2012, the United States Environmental Protection Agency (EPA) obtained authority to implement an electronic manifest program for hazardous waste shipments. Also in 2012, MAP-21 legislation authorized DOT to implement pilot studies for electronic shipping papers (e.g. electronic manifests). The project team expects that tighter chain-of-custody control resulting from an electronic manifest program will significantly reduce shipment vulnerability, especially related to insider threats. Chain-of-custody control for Tier 1 HSSM shipments, the riskiest and most dangerous shipments traveling over the roads, should be at least as tight as EPA's chain-of-custody control for hazardous waste shipments.

5 AS A PRIORITY, TSA SHOULD COMPLETE DEVELOPMENT OF AN "EMERGENCY-READY" TIER 1 HSSM SHIPMENT TRACKING/CHAIN-OF-CUSTODY SYSTEM AS QUICKLY AS POSSIBLE. THIS "EMERGENCY-READY" SYSTEM SHOULD BE READY FOR IMMEDIATE DEPLOYMENT IF TSA NEEDS TO INJECT TIGHTER SECURITY CONTROL IN THE HAZMAT SUPPLY CHAIN, ESPECIALLY IN THE AFTERMATH OF A SECURITY INCIDENT.

Currently, TSA does not have the capability to track Tier 1 HSSM shipments, nor does TSA have chain-of-custody control over Tier 1 HSSM shipments. The lack of shipment visibility (tracking) and chain-of-custody control are both serious security vulnerabilities that the project team recommends that TSA address via a regulatory program that will require Tier 1 HSSM trading partners to report data, including electronic manifest transactions, to a Public Sector Reporting Center (refer to Recommendations 1 and 2).

It will, however, take TSA about 2 1/2 years – even under an accelerated regulatory development initiative - to fully implement a Tier 1 HSSM regulatory program. In the interim, the hazmat supply chain remains vulnerable.

This vulnerability will become especially problematic if the nation suffers a security incident involving a Tier 1 HSSM shipment. If such an incident occurs, TSA will be pressured to respond quickly and aggressively to assure Congress and the nation that the hazmat supply chain is secure and that additional incidents will not occur. TSA's most likely reaction to a security incident would be to curtail or shut down Tier 1 HSSM shipments while it grapples with implementing a suitable response. Unfortunately, the impact on the economy in the event of even a short-term disruption in Tier 1 HSSM shipments would be substantial. Take, for example, the mining and heavy construction industries. Both are dependent on just-in-time delivery of explosives, a Tier 1 HSSM, and would have to curtail or cease operations if the supply of explosives to them was disrupted, even for a few days.

An even bigger problem is that TSA has few options at its disposal for quickly injecting tighter security into the Tier 1 HSSM supply chain. TSA has the authority to issue administrative security directives, but it is arguable how effective administrative security directives will be at reducing risk in the hazmat supply chain. At best, an administrative security directive will have an indirect and diffused effect on supply chain risk. Instead, TSA needs a response mechanism that allows it to directly manage risk. And, it needs a mechanism that it can implement quickly and with little disruption to the hazmat supply chain.

The project team recommends that TSA move forward – on a priority basis - on development of an "emergency-ready" version of a Tier 1 HSSM tracking/chain-of-custody system. This system would incorporate most of the functionality represented in the Public Sector Reporting Center architectural schematic in Figure IV-1 (page 42). However, there would be one key difference. The emergency–ready system would rely on a driver's GPS-enabled smart phone to serve as the telematics device to feed shipment location data into the tracking system instead of a more sophisticated truck-based telematics system. While imperfect from a telematics perspective, using a smart phone to generate shipment location data is a workable approach pending TSA regulations that will require Tier 1 HSSM carriers to deploy more sophisticated telematics systems and report shipment location data to a Public Sector Reporting Center.[2] The smart phone will also be equipped with an application to support electronic manifest (chain-of-custody) functionality.

The chief advantage of this approach is that it can be implemented quickly – almost overnight – via issuance of a security directive by TSA that would require some or all Tier 1 HSSM trading partners to use the emergency-ready system. The emergency-ready system would be ready for immediate deployment if needed and shipment tracking could begin as soon as Tier 1 shippers, carriers, and consignees register via portals and Tier 1 HSSM carriers equip their drivers with smart phones.

An emergency-ready shipment tracking/electronic manifest system – ready to be quickly put into place – is a prudent security measure that offers a powerful and immediate security upgrade in the hazmat supply chain if needed. It would give TSA the option of allowing HSSM trading partners (shippers, carriers, and consignees) to resume shipments of Tier 1 HSSMs after a security incident but with the comfort that shipment tracking and chain-of-custody controls would be in place. Also, it would allow TSA to provide Congress and the public with the assurance that it had taken tangible steps to inject tighter security into the hazmat supply chain.

It will take about a year to complete development of an emergency-ready tracking/electronic manifest system provided that TSA leverages an on-going R&D initiative. However, once developed, the emergency-ready system could be placed into service within days of an incident, substantially enhancing security in the hazmat supply chain.

If TSA elects to move forward on a Tier 1 HSSM regulatory program, the investment in the emergency-ready system will be fully leveraged as it will serve as the underlying infrastructure for a fully operational Public Sector Reporting Center. In fact, the incremental investment to convert the emergency-ready system will be relatively small, and primarily focused on refinements to ensure that system functionality supports TSA's Tier 1 HSSM regulatory requirements, especially the compliance obligations of Tier 1 HSSM trading partners.

6 BY SEPTEMBER 11, 2016, TSA SHOULD HAVE REAL-TIME VISIBILITY INTO ALL TIER 1 HSSM SHIPMENTS TRAVELING OVER THE NATION'S ROADS AND THE SYSTEMS (PSRC) CAPABILITIES IN PLACE AND OPERATING TO PROACTIVELY MANAGE RISK IN THE TIER 1 HSSM SUPPLY CHAIN.

Throughout Section VI, the project team built up a set of recommendations for TSA as it moves forward in implementing a Tier 1 HSSM shipment tracking program under Section 1554 of the 9/11 Act.

- The project team recommended that TSA implement a regulatory program in conjunction with DOT that will require Tier 1 HSSM carriers to deploy tractor- and trailer-based telematics systems and report data to a Public Sector Reporting Center (Recommendations #1 and #2).

- The project team recommended that TSA undertake a joint R&D program with DOT to build and test a Security EOBR as part of TSA's effort to encourage commercial telematics service providers to incorporate necessary security functionality into their product/service offerings and to provide TSA with

[2] Section III describes the telematics suite that the project team recommends TSA require Tier 1 HSSM carriers to deploy. Note that neither TSA nor DOT currently requires carriers to report shipment location data to a Public Sector Reporting Center. Also, neither requires Tier 1 HSSM carriers to deploy telematics systems with the full set of functionality described in Section III. In Recommendation #3, the project team suggests that TSA undertake a research & development program to build and test a prototype of the Security EOBR as a proof of concept. Note that even if the Security EOBR was currently available from commercial telematics service providers and TSA was to order immediate deployment, it would take at least several months to fully equip all Tier 1 HSSM carriers.

the data it needs to establish technology standards in a Tier 1 HSSM rule (Recommendation #3).

- The project team recommended that TSA build an emergency-ready Tier 1 HSSM shipment tracking/ chain-of-custody system on a priority basis, and that this system be refined to support an operational Public Sector Reporting Center as TSA moves forward with a Tier 1 HSSM regulatory program and as TSA completes its telematics R&D work (Recommendations #4 and #5).

The project team's final recommendation is that TSA establish **September 11, 2016,** the 15th anniversary of the attacks on the World Trade Towers and the Pentagon, as the effective date for its Section 1554 shipment tracking program. On this date, TSA should have full visibility into the movement of all Tier 1 HSSMs on the nation's roads and chain-of-custody control over all Tier 1 HSSM shipments. TSA should also have in place a Public Sector Reporting Center that will allow TSA to directly manage risk in the Tier 1 HSSM supply chain.

Action Plan

There are a number of regulatory and R&D activities that TSA would need to complete before September 11, 2016. As the project team suggests in the action plan in **Figure VI-1,** TSA would issue a Notice of Proposed Rulemaking (NPRM) by mid-2015 for a rule that will require Tier 1 HSSM carriers to deploy tractor- and trailer-based telematics systems and report data to a Public Sector Reporting Center. Concurrent with the development of its NPRM, TSA would complete and test a prototype of its Security EOBR in conjunction with DOT. Completion of the Security EOBR prototype would provide TSA with the cost and technology data it needs to support the NPRM. TSA would issue a final rule by the end of the first quarter of 2016. The final rule would establish September 11, 2016 as the rule's effective date. This six month period between the issuance of the final rule and the rule's effective date will give (1) Tier 1 HSSM carriers time to install or upgrade their telematics systems to meet TSA technical requirements as established in the final rule and (2) Tier 1 HSSM trading partners (shippers, carriers, consignees) time to register with the PSRC and adjust to TSA's regulatory requirements prior to September 11, 2016.[3]

The project team recommends that TSA build its Tier 1 HSSM emergency-ready tracking/chain-of-custody system concurrently with the drafting of the NPRM and completion of related R&D activity. The emergency –ready/chain-of custody system would be refined to match the requirements of TSA's final rule, and would be available for use by Tier 1 HSSM shippers, carriers, and consignees when TSA issues its final rule.

Critical Success Factors

Critical success factors are those things that an organization must achieve or accomplish in order to meet an important programmatic goal or objective. In this case, the programmatic objective is to "go live" with a Section 1554 HSSM shipment tracking program by September 11, 2016.

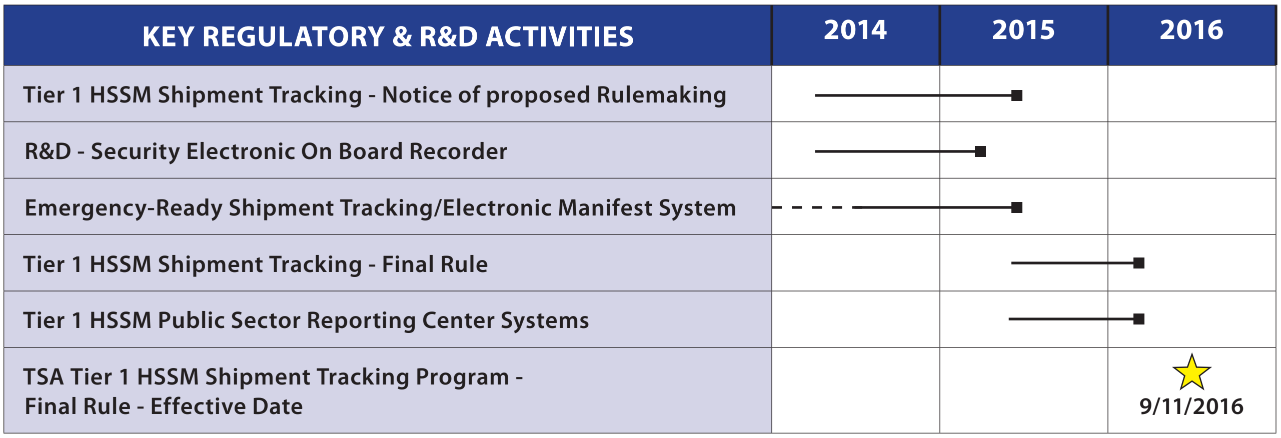


Figure VI-1. Section 1554 Program Action Plan

[3] If TSA finds the regulatory calendar proposed by the project team to be too confining, TSA might opt to issue its final Tier 1 HSSM rule on September 11, 2016 with an effective date six months later.

There are four critical success factors that are vital to TSA's success in implementing the action plan described in Figure VI-1 and in reaching its September 11, 2016 programmatic objective.

Critical Success Factor One – Programmatic Commitment

TSA must commit to development of a Tier 1 HSSM shipment tracking program as contemplated by Section 1554, and must commit to a regulatory agenda that will result in a September 11, 2016 "go-live" date for its shipment tracking program.

Critical Success Factor Two – DOT Collaboration

As required by Section 1554. TSA must consult with DOT as it develops its Section 1554 shipment tracking program. In this regard, TSA must seek out and establish a "virtuous circle" with DOT in which TSA and DOT can effectively collaborate in conducting R&D (Security EOBR) and in developing a joint Tier 1 HSSM rule.

Critical Success Factor Three – Congressional Authority

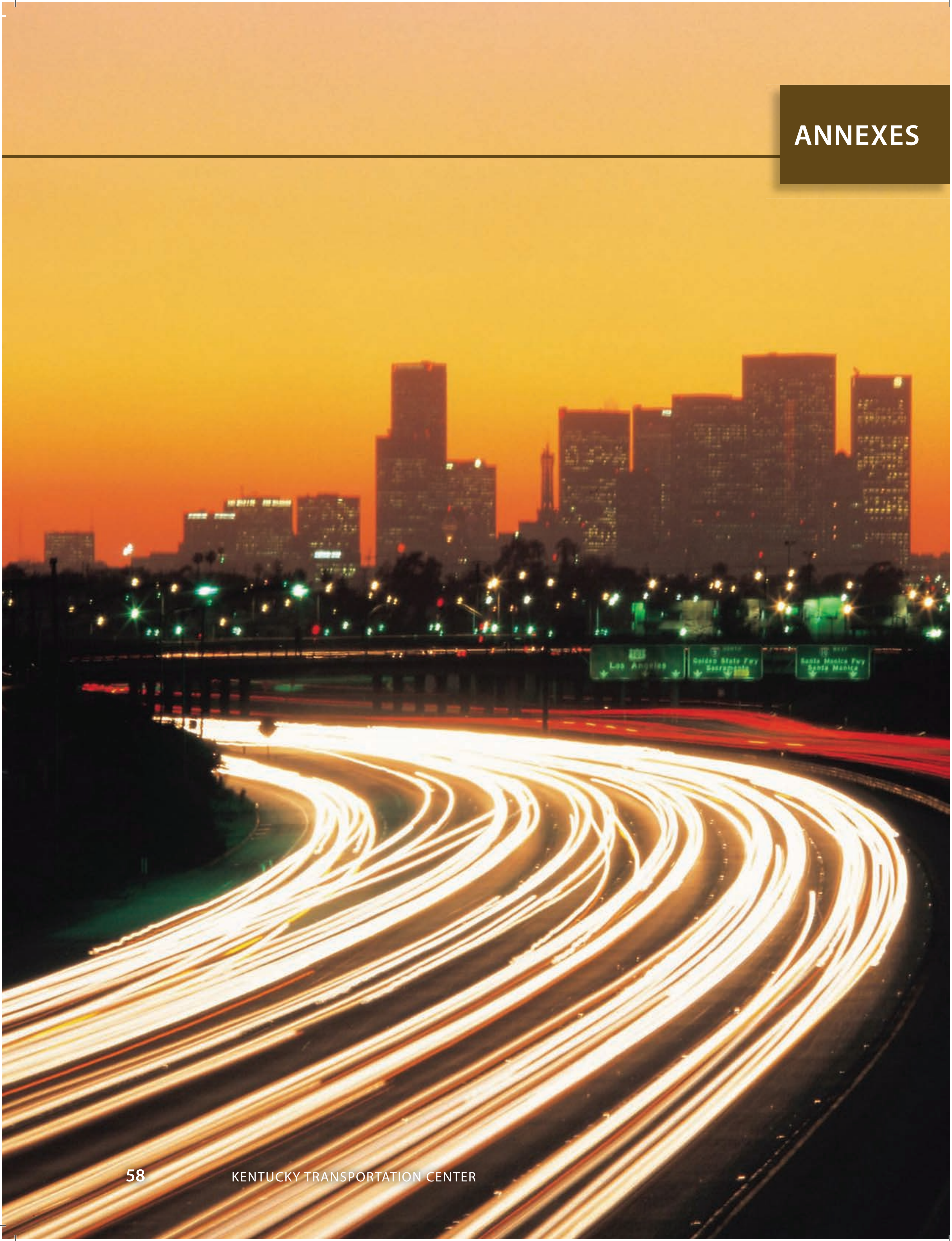
TSA must seek out and obtain Congressional authority under Section 1554(d) so that TSA can mandate the installation of telematics technology by Tier 1 HSSM carriers. TSA must have this authority in hand prior to issuance of its final rule.

Critical Success Factor Four – Investment

TSA must commit sufficient funding for full and timely completion of R&D initiatives including the Security EOBR and the emergency-ready shipment tracking/ chain-of-custody system.

• • •

ANNEXES


Los Angeles
Golden State Fwy
Sacramento
Santa Monica Fwy
Santa Monica

ANNEX A

TSA Security Action Items

En-Route Security Action Items (SAIs 10-23)

Security Action Item #10. Establish Communications Plan - 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.

Security Action Item #11. Establish Appropriate Vehicle Security Program – Employers should ensure that all company vehicles (power units including but not limited to tractors, straight trucks, pickups, and service units) are secured when unattended through use of 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.

Security Action Item #12. Establish Appropriate Cargo Security Program to Prevent Theft or Sabotage of Cargo Containers– 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

Security Action Item #13. Implement a Seal/Lock Control Program to Prevent Theft or Sabotage of Cargo – 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) developed jointly by the Department of Homeland Security and Department of Defense.

Security Action Item #14. High Alert Level Protocols – 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).~~[1] 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

[1] The Homeland Security Advisory System was phased out in 2011.

agreements with industry partners and stakeholders or utilizing state weigh stations and inspection facilities that can provide law enforcement protection.

Security Action Item #15. Establish Security Inspection Policy and Procedures – 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.

Security Action Item #16. Establish Reporting Policy and Procedures) – 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.

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.

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

ANNEX B
DOT Electronic On Board Recorders

Status: Sleeper
Start: 13:00 CDT, 07/07
Now: 03:43 CDT, 07/08
Duration: 14h 43m
Exception: None
Last (34hr) Reset: 06:12 CDT, 07/05
Next (34hr) Start: 20:12 CDT, 07/10
Hrs to be Gained: 00h 00m
Hrs Gained in 2 Days: 00h 00m
Mileage Today (mi): 0.0

EOBR Device

What are Electronic On Board Recorders?

Electronic On Board Recorders (EOBRs) are truck telematic devices fashioned to meet the requirements of DOT's Hours of Service rules. EOBRs typically involve some type of in-truck computing device that is "hard wired" to truck sensors, communicates through cellular or satellite technologies and, at the same time, provides a user interface for the driver through either a fixed screen display (e.g., mounted to the dashboard) or via a mobile device that works in sync with the on-truck device. The EOBR can then keep track of when the vehicle is moving, the location, driver and driving time details, and other information which it can record and/or send to the "back office" while also allowing the driver to enter and view information on a display. In short, EOBRs operate as conventional truck telematic devices, but packaged with software that tailors their use to the demands of DOT's HOS rules. Popular EOBR device providers, among others, include XRS, Telogis, PeopleNet, Teletrac, and Qualcomm.

DOT's EOBR experience argues that regulations will be needed to drive truck telematics technology deployment by Tier 1 HSSM carriers. DOT's Electronic On Board Recorder (EOBR) regulatory initiative is a more recent example of the need for a regulatory driver to promote technology deployment. EOBRs are basic truck telematics devices fashioned to meet the requirements of DOT's Hours of Service (HOS) rules. Longstanding DOT regulations set detailed and specific requirements that limit the HOS that a driver can remain on-duty without rest, and require drivers to maintain a log recording their HOS. For years, drivers kept paper log books, known as the driver's "record of duty status," to track their HOS.

Under its EOBR I rule (April 2010), DOT required EOBR deployment only for carriers with poor safety records. DOT had expected EOBR usage to expand well beyond the population of carriers with poor safety records, but EOBR adoption lagged prompting DOT to release its EOBR II rule less than a year later, in February, 2011, that proposed to extend the EOBR mandate throughout the trucking industry. Citing safety benefits, DOT argued that the EOBR mandate expansion was needed because "without an EOBR mandate, its [DOT's] actions have had little effect on voluntary EOBR adoption…"[1]   Only about 12% of the industry had moved to EOBRs from existing paper-based HOS logs.[2]   On July 6, 2012, MAP-21 was signed into law, increasing the force and pace of the EOBR II rulemaking. MAP-21 directed DOT to issue a final EOBR rule that will make EOBR use mandatory by mid-2015.[3]
Every major telematics service provider in the U.S. has moved to refine their product/service offerings to serve the market created by the EOBR II/MAP-21 mandate. With increased competition, the cost of EOBRs has fallen so much that DOT is now revising its EOBR regulatory cost estimates to reflect much lower market pricing.

DOT's EOBR experience serves as the strongest basis for the project team's finding that regulations will be needed to drive truck telematics technology deployment by Tier 1 HSSM carriers, and by extension, development of TSA's truck tracking program. TSA's programmatic challenge is the same as DOT's in that neither can achieve their programmatic objectives (safety, security) unless telematics technology is widely deployed in their target carrier groups. And, both DOT and TSA face similar challenges in overcoming barriers to technology deployment. Specifically, the project team drew the following out of DOT's EOBR experience.

- Like DOT, TSA will need telematics service providers to develop and sell products and services that meet its programmatic needs. So far, TSPs interviewed by

[1] DOT FMCSA, EOBR II Regulatory Impact Assessment, p. 7 (Jan., 2011).

[2] DOT FMCSA, EOBR II Regulatory Impact Assessment, p. 7 (Jan., 2011).

[3] MAP-21 Moving Ahead for Progress in the 21st Century Act, 112 P.L. 141, 32301(b) (July 6, 2012).

the project team have chosen to ignore TSA's voluntary Security Action Items (SAIs) because they have no regulatory clout to promote market interest by carriers. And without a clear statement of intent by TSA that it plans to move forward on the regulatory front, telematics service providers do not believe that a market exists for "highway security" truck telematics that justifies investment of limited corporate R&D funds. telematics service providers interviewed by the project team cited DOT's EOBR II rule as spurring on EOBR R&D investment and market competition, something that was lacking before EOBR II arose as a market driver.

- Tier 1 HSSM carriers will not widely deploy truck telematics systems or report data to a PSRC in the absence of a regulatory requirement to do so. Without widespread technology deployment, TSA's truck tracking program will fail to adequately protect the hazmat supply chain, and TSA will not capture the security benefits described in the FOT. DOT faced the same dilemma in its EOBR program. Without wide spread deployment of EOBRs by carriers, the safety benefit DOT wanted to capture in the market would have been unattainable. This prompted DOT to use a regulatory driver (EOBR II) to capture the safety benefits it wants.

DOT's EOBR I rule established performance standards and data standards for Electronic On Board Recorders.

In April 2010, after 6 years of evaluation and industry input, FMCSA published EOBR I, which (1) mandated EOBR use for the small universe of drivers who failed more than 10% of the time to comply with HOS rules, (2) set technology performance standards for EOBR technology, and (3) permitted the voluntary use of compliant EOBRs.[4] Under this rule, whether deployed voluntarily or under a "remedial mandate," EOBRs must meet (1) an enumerated list of performance standards as well as (2) data standards for the transfer and sharing of EOBR-generated data between EOBR units and government officials.

This "technology bar" for EOBRs requires, among other things, that EOBR technology (1) identify the driver prior to transit, (2) track the time when the driver is actually driving, (3) record the location of the vehicle as it moves, (4) record identifying details about the truck, (5) record details about the shipment being carried, and (6) and be capable of sharing collected data according to structured data elements and via wired and wireless methods.[5] The

[4] Electronic on-Board Recorders for Hours-of-Service Compliance, 75 Fed. Reg. 17208 (Apr. 5, 2010).

[5] 49 CFR § 395.16 (2011).

SUMMARY HIGHLIGHTS OF TECHNOLOGY PERFORMANCE STANDARDS REQUIRED UNDER EOBR I	
	EOBR TECHNOLOGY PERFORMANCE STANDARDS
Automatically Record Driving Time and "Duty Status"	• Must automatically record driving time when vehicle is in motion.
Driver Identification and Login	• Must require a user id/password, or other means such as smart cards or biometrics to identify the driver.
Record Vehicle and Shipment Information	• Must record USDOT Number of motor carrier. • Must record the truck number or tractor and trailer numbers. • Must record the shipping document number(s), or name of shipper and commodity.
Track Location of Vehicle	• While in motion, must record location at a maximum of 60-minute intervals. • During "duty status" change, must record location of nearest city, town, or village. • Location of vehicle must be derived from satellite or terrestrial sources, or a combination of both. • Must record distance traveled during on-duty driving period.
Display Functions	• Must have the capability of displaying a variety of enumerated information, including driver name, driver ID, total hours on duty, miles driven and additional data.
Performance Features	• Must give audible and visible signal when driver nears driving time limit • Must give audible and visible signal if device loses its communication signal for more than brief periods • Must allow for driver input of data only if vehicle at rest • Must not permit alteration or erasure of data collected by the EOBR
Self-Certification	• Manufacture must self-certify EOBR as meeting the requirements of the regulation.[6]

following tables highlight some of the key EOBR performance standards and data sharing standards as required by EOBR I.

DOT published data standards for location reporting and event reporting in its EOBR I rule. DOT published a flat file database model in its EOBR I rule. DOT also published a data elements dictionary that describes the data fields component of DOT's EOBR I data framework. Individual data records must be generated and recorded whenever there is a change in driver duty status, an EOBR diagnostic event (such as power-on/off, self test, etc.), or when one or more data fields of an existing data record are later amended. In the last case, the corrected record must be recorded and noted as ''current'' in the ''Event Status Code'' data field, with the original record maintained in its unedited form and noted as ''historical'' in the ''Event Status Code'' data field.[6]

[6] MAP-21's EOBR mandate requires the implementing regulations to establish a certification process, suggesting that implementing regulations will require government or 3rd-party certification rather than self-certification.

FIELDS →

RECORDS ↓

DOT'S EOBR I FLAT DATA FILE DATABASE MODEL

Person First Name	Person Last Name	Driver PIN	Event Date	Event Time	Status Code
William	Smith	978354	20050718	12:11	D
William	Smith	978354	20050718	15:17	SB
William	Smith	978354	20050718	18:53	D
William	Smith	978354	20050718	21:43	ON
William	Smith	978354	20050718	22:14	OFF
William	Smith	978354	20050719	06:25	ON
William	Smith	978354	20050719	06:47	D
William	Smith	978354	20050719	13:32	SB
William	Smith	978354	20050719	15:27	D
William	Smith	978354	20050719	20:04	SB

SUMMARY HIGHLIGHTS OF DATA REPORTING AND SHARING PERFORMANCE STANDARDS UNDER EOBR I

EOBR DATA SHARING PERFORMANCE STANDARDS	
Reporting and Sharing of Data	Must produce electronic or printed record of HOS upon demand by Federal, State, or local officials (without requiring the official to enter the vehicle)
Sharing Data via Wired Transfer	Must be capable of one-way transfer via wired communications meeting USB (Universal Serial Bus Specifications).
Sharing Data via Wireless Transfer	Must be capable of one way wireless transfer (1) meeting IEEE Std. 802.11-2007 for wireless communications, or (2) via Commercial Mobile Radio Services (CMRS) (e.g., cellular) methods.
Sharing Data Collected from "Back End" Support Systems	Home terminal support systems or 3rd-party maintained support systems must be capable of providing summaries of hours of service records as well as EOBR quality assurance information such as communication failures or edited data.
Electronic Shared Data Must Conform to Data Standards	Data required to be recorded and shared must be structured in a flat file database conforming to the data elements specified in EOBR I – which lists 29 data elements for data in the following categories: • Drivers • Vehicles • Carrieers • Shipments • Events (duty status, date, time, location, etc.)

EOBR DATA ELEMENTS DICTIONARY

DATA ELEMENT	DATA ELEMENT DEFINITION	TYPE	LENGTH	VALID VALUES AND NOTES
DRIVER IDENTIFICATION DATA				
Driver First Name	First name of the driver	A	35	See Note 1.
Driver Last Name	Last name, family name, or surname of the driver	A	35	See Note 1.
Driver PIN/ID	Numeric identification number assigned to a driver by the motor carrier	A	40	
VEHICLE IDENTIFICATION DATA				
Tractor Number	Motor carrier assigned identification number for tractor unit.	A	10	
Trailer Number	Motor carrier assigned identification number for trailer	A	10	
Tractor VIN Number	Unique vehicle ID number assigned by manufacturer according to US DOT regulations.	A	17	
CO-DRIVER DATA				
Co-Driver First Name	First name of the co-driver	A	35	See Note 1.
Co-Driver Last Name	Last name, family name, or surname of the co-driver	A	35	See Note 1.
Co-Driver PIN/ID	Numeric identification number assigned to a driver by the motor carrier	A	40	
COMPANY IDENTIFICATION DATA				
Carrier USDOT Number	USDOT Number of the motor carrier assigned by FMCSA.	N	8	
Carrier Name	Name or trade name of the motor carrier company appearing on the Form MCS–150.	A	120	
SHIPMENT DATA				
Shipping Document Number	Shipping document number	A	40	
EVENT DATA				
Event Sequence ID	A serial identifier for an event that is unique to a particular vehicle and a particular day.	N	4	0001 through 9999.

Event Status Code	Character codes for the four driver duty status change events, State border crossing event, and diagnostic events.	A	3	OFF = Off Duty
				SB = Sleeper Berth
				D = On Duty Driving
				ON = On Duty Not Driving
				DG = Diagnostic

Event Date	The date when an event occurred	N (Date)	8	UTC (universal time) recommended. Format: YYYYMMDD.
Event Time	The time when an event occurred	N	6	UTC (universal time) recommended. Format: HHMMSS (hours, minutes, seconds).

EOBR DATA ELEMENTS DICTIONARY				
DATA ELEMENT	DATA ELEMENT DEFINITION	TYPE	LENGTH	VALID VALUES AND NOTES
EVENT DATA				
Event Latitude	Latitude of a location where an event occurred	N	2,6	Decimal format: XX.XXXXXX.
Event Longitude	Longitude of a location where an event occurred	N	3,6	Decimal format: XXX.XXXXXX.
Place Name	The location codes must correspond, at a minimum, to ANSI INCITS 446–2008, "American National Standard for Information Technology—Identifying Attributes for Named Physical and Cultural Geographic Features (Except Roads and Highways) of the United States, Its Territories, Outlying Areas, and Freely Associated Areas and the Waters of the Same to the Limit of the Twelve-Mile Statutory Zone (10/28/2008)," where "GNIS Feature Class" = "Populated Place" (incorporated by reference, see § 395.18). (For further information, see also the Geographic Names Information System (GNIS) at http://geonames.usgs.gov/domestic/index.html.	N	5	Unique within a FIPS state code. Lookup list derived from GNIS.
Place Distance Miles	Distance in miles to nearest populated place from the location where an event occurred.	N	4	
Total Vehicle Miles	Total vehicle miles (as noted on vehicle odometer or as measured by any other compliant means such as vehicle location system, etc.).	N	7	With total vehicle mileage recorded at the time of each event, vehicle miles traveled while driving, etc., can be computed.

Event Update Status Code.	A status of an event, either Current (the most up-to-date update or edit) or Historical (the original record if the record has subsequently been updated or edited).	A	1	C = Current,
				H = Historical.

Diagnostic Event Code.	For diagnostic events (events where the "Event Status Code" is noted as "DG"), records the type of diagnostic performed (e.g., power-on, self-test, power-off, etc.).	A	2	(See Table 3).
Event Error Code	Error code associated with an event	A	2	(See Table 3).
Event Update Date	The date when an event record was last updated or edited.	N (Date)	8	UTC (universal time) recommended. Format: YYYYMMDD.
Event Update Time	The time when an event record was last updated or edited.	N	6	UTC (universal time) recommended. Format: HHMMSS (hours, minutes, seconds).
Event Update Person ID.	An identifier of the person who last updated or edited a record.	A	40	
Event Update Text	A textual note related to the most recent record update or edit.	A	60	Brief narrative regarding reason for record update or edit.

EOBR DIAGNOSTIC EVENT CODES

Code class	Code	Description	Full Description
General System Diagnostic	PWR_ON	Power on	EOBR initial power-on
General System Diagnostic	PWROFF	Power off	EOBR power-off
General System Diagnostic	TESTOK	test okay	EOBR self test successful
General System Diagnostic	SERVIC	Service	EOBR Malfunction (return unit to factory for servicing)
General System Diagnostic	MEMERR	memory error	System memory error
General System Diagnostic	LOWVLT	Low voltage	Low system supply voltage
General System Diagnostic	BATLOW	battery low	EOBR system clock error (clock not set or defective)
General System Diagnostic	CLKERR	clock error	EOBR system clock error (clock not set or defective)
General System Diagnostic	BYPASS	Bypass	EOBR system bypassed (RODS data not collected)
Data Storage Diagnostic	INTFUL	internal memory full	Internal storage memory full (requires download or transfer to external storage)
Data Storage Diagnostic	DATACC	Data accepted	System accepted driver data entry
Data Storage Diagnostic	EXTFUL	external memory full	External memory full (smartcard or other external data storage device full)
Data Storage Diagnostic	EXTERR	external data access error	Access external storage device failed
Data Storage Diagnostic	DLOADY	download yes	EOBR data download successful
Data Storage Diagnostic	DLOADN	download no	Data download rejected (unauthorized request/wrong Password).
Driver Identification Issue	NODRID	no driver ID	No driver information in system and vehicle is in motion
Driver Identification Issue	PINERR	PIN error	Driver PIN/identification number invalid
Driver Identification Issue	DRIDRD	Driver ID read	Driver information successfully read from external storage device (transferred to EOBR).
Peripheral Device Issue	DPYERR	display error	EOBR display malfunction
Peripheral Device Issue	KEYERR	keyboard error	EOBR keyboard/input device malfunction
External Sensor Issue	NOLTLN	no latitude longitude	No latitude and longitude from positioning sensor
External Sensor Issue	NOTSYC	no time synchronization	Unable to synchronize with external time reference
External Sensor Issue	COMERR	communications error	Unable to communicate with external data link (to home office or wireless service provider).
External Sensor Issue	NO_ECM	no ECM data	No sensory information received from vehicle's Engine Control Module (ECM)
External Sensor Issue	ECM_ID	ECM ID number mismatch	ECM identification/serial number mismatch (with preprogrammed information).

ANNEX C
Benefits: Tier 1 HSSM Shipment Tracking Program

FMCSA’s Hazardous Materials Safety and Security Operational Field Test (FOT) was a seminal study examining the use of truck telematics technology to enhance hazmat shipment safety and security. It was the first and only large-scale test of truck telematics technology, and is particularly notable because the FMCSA project team quantified the costs and benefits associated with telematics technology deployment by hazmat carriers.

The study quantified three types of benefits: operational efficiency benefits, safety benefits, and security benefits.

Operational Efficiency Benefits

Truck telematics systems save carriers money by making their operations more efficient – routing is more efficient, scheduling is more efficient, and less fuel is consumed. Most large, long-haul carriers have already installed truck telematics systems offered from telematics service providers such as Qualcomm and PeopleNet. The FOT project team estimated the unit cost operational efficiency benefits associated with the deployment and use of truck telematics systems.[1] As illustrated in **Figure C-1**, the FOT estimated that a typical bulk chemicals carrier would save $7,116/truck/year after deploying a basic truck telematics system. An explosives carrier would save $10,968/truck/year.[2] Most bulk chemicals and explosives are Tier 1 Highway Security Sensitive Materials.

Notably, cost savings are sensitive to the cost of fuel. Since late 2004 when the FOT was completed, the cost of diesel fuel has more than doubled – from about $1.75/gallon to about $4/gallon today. This means that the numbers in the table below are conservative estimates of the unit cost savings a carrier would realize today.

Quick ROI does not mean that carriers will invest in telematics systems, however. The FOT project team concluded that a regulatory driver will be needed to promote wide-scale deployment of truck telematics systems and data reporting to a centralized tracking facility, both requisites for a successful truck tracking program. In particular, the report was clear that the majority of hazmat carriers would not deploy truck telematics systems in the absence of a regulatory requirement to do so – even though truck telematics systems generate significant cost savings for carriers.

“… Even with attractive return-on-investment (ROI) and low

[1] FMCSA Hazmat Safety and Security Technology Field Operational Test http://www.fmcsa.dot.gov/safety-security/hazmat/fot/eval-rpt-synthesis-intro.htm - pages 39-45

[2] Table 5-2, page 43 FMCSA Hazmat Safety and Security Technology Field Operational Test

TELEMATICS AND OPERATIONAL BENEFIT

Operational Benefits	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	$253/month a. $19 b. $122 c. $37 d. $65 e. $11	$491/month a. $30 b. $81 c. $290 d. $78 e. $13
Improved Maintenance Scheduling • Reduces maintenance & repair cost • Increases revenue miles by reducing downtime	$18/month	$37/month
Reduce Out-Of-Route Mile • Creates savings of line haul variable costs	$123/month	$116/month
Improved Vehicle Utilization by Reducing Empty Miles • Increases potential number of trips	$199/month	$270/month
Total Monthly Benefit Per Truck	$593/month	$914/month
Total Annual Benefit Per Truck	$7,116/year	$10,968/year

Figure C-1.

> 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."

In a related issue, the FOT project team also concluded that the highway hazmat security program would fail without wide scale technology deployment.

> "It should be noted that partial deployment might not necessarily result in a directly proportional security benefit. In other words, 50 percent deployment may not yield 50 percent of achievable security benefits. This may occur because while the technology-equipped fleet may not be attacked, a non-equipped fleet would possibly be targeted instead. The deterrent effect of the technologies, if partly deployed, could simply shift terrorist targeting from one fleet to another, with no net change in overall security. Under this assumption, then full deployment is required to realize the security benefits."

Cost reduction from operational efficiency is the key value proposition that telematics service providers offer their customers. The FOT finding about the purchasing behavior of carriers was reaffirmed by the project team as it met with prominent telematics service providers during the Section 1554 study. Every telematics service provider interviewed by the project team uses a ROI sales approach for their telematics/fleet management products and services. Each had compelling data/sales information that proved that their products/services generate very rapid ROI – ranging from a few months to less than a year. Almost universally, the telematics service providers lamented that many carriers refuse to spend the money on telematics even in the face of clear evidence that the investment will pay off quickly in the form of lower operating costs. All the telematics service providers were in agreement with the FOT conclusion that only a regulatory driver will prompt wide-scale deployment of telematics systems in any carrier group, including Tier 1 HSSM carriers.

Security Benefits

The FMCSA Hazmat Safety and Security Technology Operational Field Test quantified security benefits associated with the deployment of truck telematics systems and the implementation of a centralized tracking system.[3]
A detailed and comprehensive methodology was used to quantify security benefits in the FOT. Essentially, a panel of subject matter experts determined vulnerability reduction that would be captured by deploying various combinations of telematics equipment on trucks. Security benefit was calculated by multiplying vulnerability reduction by reasonable worst case consequences.

Figure C-2 summarizes resulting security benefit calculations. The figure was drawn directly from the FOT report. The last two telematics packages in the table (highlighted text) are closest to the type of telematics portfolio that TSA might require in its highway hazmat security program.

The primary evaluation objective of the Security Benefits Assessment in FMCSA's Hazardous Materials Safety and Security Operational Field Test was to examine the ability of the truck telematics to improve shipment security. The project team did this by quantifying how telematics

TELEMATICS REDUCE SHIPMENT VULNERABILITY; GENERATE SECURITY BENEFITS

Telematics Technology Package	Vulnerability Reduction %		Securit y Benefit (in Millions of Dollars)	
	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) + GPS Position	16%	12%	$2,581	$1,657
WC + GPS Position + Panic Alert	25%	21%	$4,058	$2,822
WC + GPS Position + Shipment Tracking (PSRC)	24%	20%	$3,891	$2,652
WC + GPS Position + Vehicle Disabling + Panic Alert	31%	25%	$5,098	$3,355
WC + GPS Position + Panic Alert + Driver ID + Manifest	33%	26%	$5,319	$3,510

Figure C-2.

[3] FMCSA Hazmat Safety and Security Technology Field Operational Test http://www.fmcsa.dot.gov/safety-security/hazmat/fot/eval-rpt-synthesis-intro.htm - pages 47-60

technology – in coordination with reasonable security processes and procedures – would reduce security vulnerabilities in truck-based hazmat shipping. The bottom line of the FMCSA study was a quantification of net consequences avoided (security benefits) if a given technology or set of technologies were deployed by hazmat carriers. The project team was intent on being able to draw conclusions such as, if all bulk chemical carriers are equipped with baseline telematics (GPS and wireless modem), panic buttons, and vehicle disabling telematics, the security benefit – due to a reduction in security vulnerability - would be $5.098 billion.

As the FOT report pointed out, quantifying the potential security impacts (consequence reduction) related to the use of telematics was difficult because there was little or no event data on which to reliably baseline the level of hazmat-based terrorist attacks or to provide actuarial data in which to predict a statistically significant number of actual terrorist actions in the future. The FOT project team had to develop a method that would translate field test performance and user acceptance information into monetized risk reduction terms. A summary of the approach used by the FOT project team follows.

The FOT was completed in 2004. However, the security benefits findings from the study are still valid today and are relevant to cost/benefits deliberations in the Section 1554 study.

The security benefits methodology in FMCSA's Hazardous Materials Safety and Security Operational Field Test mewas sophisticated, comprehensive, and consistent with current DHS risk approaches. The FMCSA project team employed a sophisticated and comprehensive approach to quantifying benefits, especially security benefits. The methodology was based on the 'threat, vulnerability, consequence' risk approach in use today at DHS as well as specific threat scenarios that TSA has incorporated into its highway program. A large group of subject matter experts from industry and government fed their expertise into the Hazardous Materials Safety and Security Operational Field Test.

Explosives and bulk chemicals are Tier 1 HSSMs. The Hazardous Materials Safety and Security Operational Field Test was completed before TSA issued its list of Tier 1 HSSMs – the riskiest materials on the nation's roads. However, two groups of hazardous materials studied – explosives and bulk chemicals – are Tier 1 HSSMs. As "pure play" Tier 1 HSSMs, conclusions reached by the FMCSA project team in terms of benefits for these materials are applicable to TSA's present day highway hazmat security program.

Security benefits are likely understated. The Hazardous Materials Safety & Security Operational Field Test quantified security benefits using the standard DOT/DHS risk equation in which Risk (cost) = threat x vulnerability x consequence. In general, the security benefit is a function of the amount of vulnerability reduction that telematics systems offer for explosives shipments or bulk chemical shipments. Vulnerability reduction in the study is likely understated – perhaps significantly so – in relation the vulnerability reduction that TSA might capture with an enhanced "security" telematics package, tighter chain-of-custody control via an electronic manifest program, and closer shipment monitoring via centralized shipment tracking.

FMCSA Security Benefits Assessment Overview

Because of the difficulties of quantifying impacts, the FOT project team built a sophisticated analytical framework to assess potential benefits. This framework built on the traditional vulnerability assessment techniques complemented by extensive input from subject matter experts. The core of the framework is expressed by the classic vulnerability assessment equation.

Cost = Threat x Vulnerability x Consequence

COST - the financial impact of hazmat-based terrorist attacks

THREAT—the relative attractiveness of a shipment (to a terrorist)

VULNERABILITY—the likelihood of a successful attack

CONSEQUENCE—the magnitude of a successful attack

The FOT project team could apply this formula to determine 'cost' before and after the deployment of different types/combinations of telematics technologies. This allowed the FOT team to quantify security benefits in economic terms.

Figure C-3 illustrates the process that the FOT project team followed in assessing security benefits. As the figure shows, the process was comprehensive. To begin the technology benefits assessment, typical hazmat motor carrier operational scenarios were identified and the most likely terrorist attack profiles for each of these scenarios were developed. For example, a typical operational scenario may be the delivery of a bulk chemical. A possible associated attack profile for this load and shipment scenario could be the use of a falsified manifest to divert the shipment to a populated area for intentional release. The four key operational scenarios or load types consid-

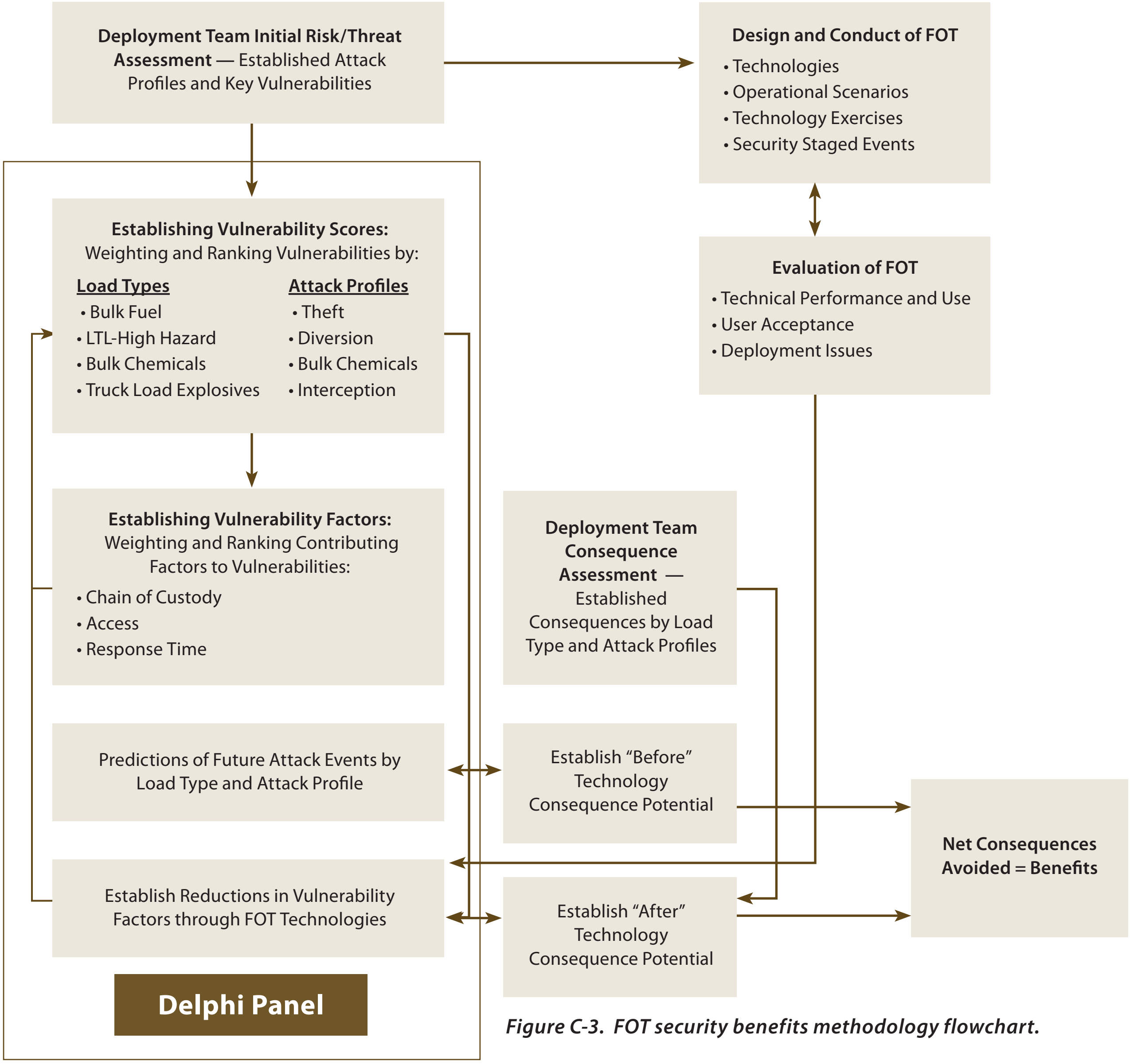

Deployment Team Initial Risk/Threat Assessment — Established Attack Profiles and Key Vulnerabilities
Design and Conduct of FOT
• Technologies
• Operational Scenarios
• Technology Exercises
• Security Staged Events
Establishing Vulnerability Scores: Weighting and Ranking Vulnerabilities by:
Load Types
• Bulk Fuel
• LTL-High Hazard
• Bulk Chemicals
• Truck Load Explosives
Attack Profiles
• Theft
• Diversion
• Bulk Chemicals
• Interception
Evaluation of FOT
• Technical Performance and Use
• User Acceptance
• Deployment Issues
Establishing Vulnerability Factors: Weighting and Ranking Contributing Factors to Vulnerabilities:
• Chain of Custody
• Access
• Response Time
Deployment Team Consequence Assessment — Established Consequences by Load Type and Attack Profiles
Predictions of Future Attack Events by Load Type and Attack Profile
Establish "Before" Technology Consequence Potential
Net Consequences Avoided = Benefits
Establish Reductions in Vulnerability Factors through FOT Technologies
Establish "After" Technology Consequence Potential
Delphi Panel

Figure C-3. FOT security benefits methodology flowchart.

ered under the FOT were: Bulk Fuel, Less-than-Truckload High Hazard, Bulk Chemicals, and Truckload Explosives. (For our purposes, only two load types are relevant: bulk chemicals and truckload explosives, both Tier 1 HSSMs.)

Numerous operational scenarios and profiles were built in an earlier study. An example of such a scenario would be the theft of a truck carrying explosives while en route, driven to a populated area and detonated to maximize casualties. For each operational scenario and attack profile, the project team evaluated 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. A key early determination was that threats would not be impacted by the technologies deployed in the FOT. Deployment of a technology or set of technologies 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 assessment.

Once the FOT project team determined that threat was a constant value, the team moved on to an evaluation of the weight and rank of **vulnerabilities**. These vulnerabilities represent the probability that a given attack profile varies given potential weaknesses in the various stages and processes involved in transporting hazmat from shipper to consignee. Vulnerabilities may include physical security gaps, information integrity lapses, operational failings, and environmental factors that are favorable to terrorist goals. These vulnerabilities were defined by the project team and consolidated into higher-level categories.   Once the "before" vulnerabilities were assessed, the project team determined the impact of telematics technology to address the vulnerabilities.

Finally, the project team evaluated the likely consequence of a success for a given attack profile and hazmat operational scenario. In the study, the consequence estimates represented aggregate numbers that include societal impacts - lost wages, damage to infrastructure, and loss of human life - as represented by economic values. Again, these values were determined in a previous effort performed by the project team. As with the threat element of the vulnerability assessment formula, the consequence of a successful attack did not change as a result of the technology deployment. This means that in the risk equation, only V (vulnerability) varies, threat and consequence are constants.

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 considered technology countermeasure for each load type.

The Evaluation Team used two distinct groups of subject matter experts in developing the Security Assessment framework: an **Expert Panel** and a **Delphi Panel**. These two panels further provided input to derive the initial vulnerability values, the potential technology enabled vulnerability reductions, and the likelihood of attacks by terrorists using truck-based HAZMAT shipments.

The Expert Panel was a core advisory group consisting of 16 project-sponsored or volunteer experts in hazmat transportation, national security, risk and loss prevention, and public safety.

The Delphi Panel supporting the security benefits assessment was comprised of 26 expert individuals, who were highly knowledgeable experts in the subject of security, risk assessment, emergency response, and enforcement as pertaining to HAZMAT shipping.

The Delphi Method is a widely used practice for transportation vulnerability assessment. Through the use of a Delphi Method, experts were asked to provide estimates of vulnerability and of the beneficial effects of the FOT-considered technologies. These inputs were collected via surveys. Both numerical and linguistic responses were developed over a series of group interrogations. Outputs with linguistic values were then processed using Soft Computing Methods in order to provide input values that support conventional Multi-Attribute Decision Making Methods.

FMCSA Vulnerability and Technology-Enabled Vulnerability Reductions

Three attack profiles were considered by the Delphi Panel for each load type.

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.

Contributing to the potential success of an attack, three Vulnerability Factors (VF) were evaluated by the Delphi Panel:

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 form 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 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) varies 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.

In establishing the "before" or "no technology" baseline, the Delphi Panel was surveyed to evaluate the vulnerability of each shipment type against each attack type in a structured format. The panelists assigned a Vulnerability Score (VS) to each of the shipments considered in the FOT for each attack type. The panelists were asked to assign a value in a range using a rating scale from 0.0 to 10.0 (in which 0.0 is extremely low and 10.0 is extremely high). This value, the VS, served three purposes to:

Establish the vulnerability for a shipment to an attack type (theft, diversion, or interception).

Establish the Panelists' estimate of the relative vulnerability among all shipment types to a particular attack type.

Establish the Panelists' estimate of the relative severity among threats.

The Panelists then estimated the contribution of each VF to the VS for each shipment type. This is done by assigning a "weight" (in terms of percentage) to each VF (chain of custody, access, and response time), indicating the Panelists' judgments on the degree of influence each factor has on the overall vulnerability of a shipment type to a specific attack type. The Panelists' judgments are made based on evaluation of the baseline information, or pre-technology condition.

The before (no technology) and after (with technology) impacts of technology on these Delphi Panel-weighted vulnerability factors were incorporated into calculations of the overall probability of attack success reductions. The weighted sum mean reductions in probability of success for each of the attack types, by load type, and by technology countermeasure, are presented in **Figure C-4**. These were derived by averaging the technology-enabled reductions in vulnerability of the contributing VFs, weighted by the contribution of each VF to the attack types. The relative likelihood of attack methods and the weighting of vulnerabilities/vulnerability subcomponents assigned to the load types by the Delphi Panel were used to develop overall vulnerability reduction for the technologies by load type. The average vulnerability reductions weighted by the VSs for each load type are presented in **Figure C-5**.

Vulnerability reductions from 0-10 percent are considered negligible; reductions from 11-25 percent are considered low; reductions from 26-50 percent are considered medium; and greater than 50 percent is considered a high reduction.

FMCSA Security Benefits Calculation

Multiplying overall vulnerability reduction of a telematics technology package by the potential consequences of an attack provides a direct estimate of potential security benefits afforded by the technology package.

For the Security Assessment, benefits were defined as potential reductions in the costs through full deployment of the technologies. These represent societal benefits. The "per event" potential consequences of hazmat-based attacks

VULNERABILITY REDUCTION VARIES BY ATTACK TYPE.

TELEMATICS TECHNOLOGY PACKAGE	% REDUCTION IN VULNERABILITY OF THEFT		% REDUCTION IN VULNERABILITY OF DIVERSION		% REDUCTION IN VULNERABILITY OF INTERCEPTION	
	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) + GPS Position	27%	20%	14%	13%	6%	7%
WC + GPS Position + Panic Alert	42%	33%	23%	23%	9%	12%
WC + GPS Position + Shipment Tracking (PSRC)	39%	31%	22%	22%	10%	11%
WC + GPS Position + Vehicle Disabling + Panic Alert	52%	40%	29%	27%	12%	14%
WC + GPS Position + Panic Alert + Driver ID + Manifest	55%	42%	30%	29%	12%	14%

Figure C-4.

VULNERABILITY REDUCTION VARIES BY LOAD TYPE.

TELEMATICS TECHNOLOGY PACKAGE	% REDUCTION IN OVERALL VULNERABILITY BY LOAD TYPE AND TECHNOLOGY	
	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) + GPS Position	16%	12%
WC + GPS Position + Panic Alert	25%	21%
WC + GPS Position + Shipment Tracking (PSRC)	24%	20%
WC + GPS Position + Vehicle Disabling + Panic Alert	31%	25%
WC + GPS Position + Panic Alert + Driver ID + Manifest	33%	26%

Figure C-5.

were obtained from an earlier FMCSA study by Battelle that explored the potential economic impacts of intentional and non-intentional releases of hazmat.[4] The study examined the potential consequences as measured by:

- 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 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 or supplies cannot be received, or other constraints imposed by the incident.

The estimates of the consequences of intentional releases of hazmat were derived through a framework that developed a series of multipliers to estimate the overall economic impacts of hazmat releases based on likely numbers of human casualties. The multipliers were based on a proxy measure for estimating effects. As the study states:

> "Fires were considered a reasonable proxy in that a large-scale hazardous materials incident often includes a fire and/or explosion, affecting multiple residences/businesses and resulting in traffic delays and community disruption."

Using these multipliers with estimated casualties for intentional hazmat releases based on load type, quantity and attack scenarios and reasonable worst-case consequence estimates were developed.

The Battelle study presented reasonable worst-case consequence estimates for hazmat classes. Derivation of the per event consequence values used in the FOT assessment considered the composition of hazmat for each load type, potential quantities released (TL versus LTL) and the Delphi Panel predicted distribution of attacks with undirected versus directed (including detonation) releases. The Panel arrived at the per-attack consequence estimates presented in **Figure C-6**.

To put these consequence numbers into context, the following examples of the consequences of terrorist attacks in the United States were offered.

- 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 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.

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

REASONABLE WORST-CASE HAZMAT ATTACK CONSEQUENCES	
FOT LOAD TYPE	REASONABLE WORST-CASE HAZMAT ATTACK CONSEQUENCES
Bulk Chemicals	$16.3 Billion
Truckload Explosives	$13.3 Billion

Figure C-6.

Although threat may vary over time and is difficult to predict, in estimating the security benefit, threat was 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. By holding threat constant, ***the security benefits of the technologies were derived using the overall vulnerability reductions multiplied by the consequences of hazmat-based terrorist attacks.*** For example, the benefit calculated for Wireless Communications with GPS positioning for Bulk Chemicals is calculated as follows:

Security Benefit = (Bulk Chemical Consequence) X (Technology Vulnerability Reduction)
Security Benefit = $16.3 Billion Consequence X 16% Vulnerability Reduction from Wireless Communications/GPS Positioning

Security Benefit = $2.6 Billion

The estimated security benefits associated with varying telematics configurations are presented in **Figure C-7**. The last telematics package in the table (highlighted text) is closest to the type of telematics portfolio that TSA might require in its highway hazmat security program. Deployment of this telematics package will generate over $5.3 Billion in security benefits.

The security benefit associated with a shipment tracking center exceeds $1 Billion. As illustrated in **Figure C-8,** the security benefit of shipment tracking can be isolated by comparing security benefits for a basic telematics setup (WC + GPS) with a setup that includes the basic telematics package and shipment tracking.

SECURITY BENEFITS FROM TELEMATICS DEPLOYMENT				
TELEMATICS TECHNOLOGY PACKAGE	VULNERABILITY REDUCTION %		SECURIT Y BENEFIT (in Millions of Dollars)	
	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives
Wireless Communications (WC) + GPS Position	16%	12%	$2,581	$1,657
WC + GPS Position + Panic Alert	25%	21%	$4,058	$2,822
WC + GPS Position + Shipment Tracking (PSRC)	24%	20%	$3,891	$2,652
WC + GPS Position + Vehicle Disabling + Panic Alert	31%	25%	$5,098	$3,355
WC + GPS Position + Panic Alert + Driver ID + Manifest	33%	26%	**$5,319**	$3,510

Figure C-7.

SECURITY BENEFITS OF CENTRALIZED SHIPMENT TRACKING			
TELEMATICS TECHNOLOGY PACKAGE		SECURITY BENEFIT - BULK CHEMICALS	SECURITY BENEFIT - TRUCKLOAD EXPLOSIVES
	WC + GPS Position + Shipment Tracking	$3,891	$2,652
Less	WC + GPS Position	$2,581	$1,657
Equals	Shipment Tracking	$1,310	$995

Figure C-8.

ANNEX D
Cost Assumptions: Tier 1 HSSM Shipment Tracking Program

The project team estimated the cost of deploying and operating tractor- and trailer-based telematics systems in the context of an overall regulatory program that requires Tier 1 HSSM carriers to deploy telematics equipment and report data to a centralized shipment tracking center. The team needed to make a number of assumptions to compile costs.

- How many Tier 1 HSSM shipments are there per year?
- What is the unit capital cost for tractor- and trailer- based telematics systems?
- What is the annual operating cost of tractor- and trailer-based telematics systems?
- How many tractors or straight trucks need to be equipped with telematics equipment?
- How many trailers need to be equipped with telematics equipment?
- What is the compliance cost of a Tier 1 HSSM regulatory program?
- What is the cost of establishing and operating a shipment tracking center?

The project team summarized costs into three categories: 1) telematics capital and operating costs; 2) compliance costs; and 3) centralized shipment tracking costs. Project team cost assumptions are presented in the following sections, followed by a summary of project team cost findings.

Telematics Capital and Operating Costs

Number of Tier 1 HSSM Shipments per Year. According to TSA's Trucking and Hazardous Materials Trucking Risk Assessment (2010), there were 1,892,532 Tier 1 HSSM shipments in 2005.[1] For purposes of this analysis, the project team rounded up the number of Tier 1 HSSM shipments to 2 million/year. Given 300 operating days per year, this would mean that there are about 6,750 trucks hauling Tier 1 HSSM shipments on the road every day.[2]

Number of Tier 1 HSSM Telematics Units. Straight trucks (no tanker/trailer) account for about a quarter of the vehicles that haul Tier 1 HSSM shipments.[3] So of the 6,750 vehicles on the road hauling Tier 1 HSSMs on any day, about 1,750 are straight trucks and 5,000 are tractors pulling a trailer or a tanker. Straight trucks, of course, will not require a trailer telematics system.

Figure D-1 illustrates trailers that are typically used in the transport of Tier 1 HSSMs. The general industry rule of thumb is that a carrier will operate 2.5 trailers/tankers for every tractor. This means that Tier 1 HSSM carriers will need to deploy about 12,500 trailer telematics units.

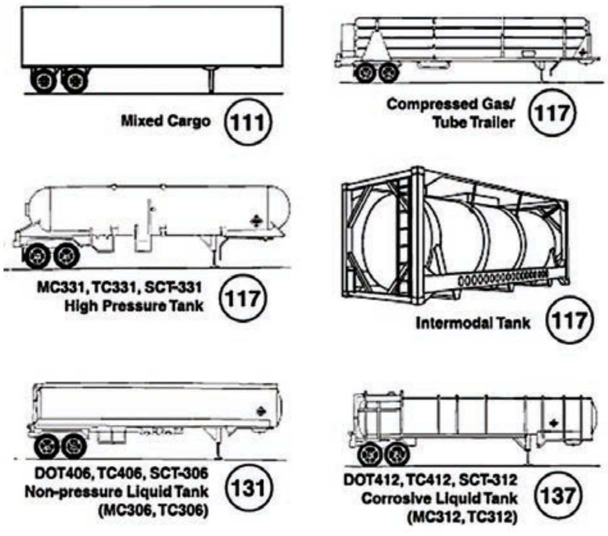

Mixed Cargo
111
Compressed Gas/ Tube Trailer
117
MC331, TC331, SCT-331 High Pressure Tank
117
Intermodal Tank
117
DOT406, TC406, SCT-306 Non-pressure Liquid Tank (MC306, TC306)
131
DOT412, TC412, SCT-312 Corrosive Liquid Tank (MC312, TC312)
137

Figure D-1. Tier 1 HSSM trailers - DOT classification.
Source: DOT Emergency Response Guide

According to Frost & Sullivan, about 15% of trailers in the U.S. are equipped with trailer telematics system and trailer telematics market deployment will grow to about 20% by 2017.[4] The actual percentage of Tier 1 HSSM carriers that deploy trailer telematics systems is higher than the average of 15% – perhaps much higher. However, data is lacking on trailer telematics deployment data for Tier 1 HSSM carriers. The project team assumed that only 15% of Tier 1 HSSM carriers have deployed trailer telematics system, the national average for all trailers/tankers carrying all

[1] TSA Trucking and Hazardous Materials Trucking Risk Assessment (THTRA); July 30, 2010; page 115.

[2] Page 116

[3] FMCSA analysis of 2005 MCMIS data; percentage of straight trucks that carry materials subject to FMCSA hazmat safety permits.

[4] Frost & Sullivan, Trailer Telematics Market: Overview of Trailer Telematics (North America), 2010.

material load types. The estimate of the number of trailer telematics systems needed in Tier 1 HSSM carrier fleets is reduced by 15%, or 1,875 units, to 10,625 to account for trailers that have already installed trailer tracking telematics systems, as illustrated in **Figure D-2**. Existing trailer telematics systems are expected to meet TSA's trailer tracking requirements.

Capital and Operating Cost – Tractor Telematics Units. The project team recommends that TSA adopt a telematics strategy that involves leveraging the DOT EOBR initiative by seeking deployment of a "Security EOBR" by Tier 1 HSSM carriers. DOT's EOBR is a basic telematics device in that it is integrated with a tractor's engine/sensor network and is capable of reporting out vehicle location. While this limited telematics functionality will not fully meet TSA's needs, JBUS integration and GPS/location reporting are both core functions that TSA needs in a telematics security solution. A Security EOBR would be able to serve both DOT's EOBR needs as well as TSA's additional telematics needs.

Telematics service providers have responded heartily to DOT's electronic on board recorder/hours of service rule. Originally, DOT planned to require only carriers with poor safety scores to implement EOBR/HOS systems. An update to DOT's EOBR rule will require almost every commercial vehicle, and all Tier 1 HSSM carriers, to implement EOBR/HOS by mid-2015. This represents a tangible growth opportunity for U.S. telematics service providers. While most of the telematics service providers already accommodate HOS functionality in their product/service offerings, all are looking to final DOT requirements to refine their services to support DOT's EOBR/HOS requirements. The EOBR/HOS competition will be greatest for medium-size carriers that will install telematics systems for the first time or upgrading telematics functionality beyond basic "track and trace" functionality.

In using the DOT (safety) EOBR as a foundational device for the Security EOBR, TSA will be able to draw on DOT's work in defining technology standards for the EOBR. In Section II of this report, the project team focused on defining incremental functionality that would need to be built into the DOT EOBR to enhance it to meet TSA's security functionality requirements.

In its EOBR II rule, DOT estimated the cost of an EOBR device at $1,625 plus monthly operating costs. When annualized along with monthly operational costs, DOT's EOBR annual cost estimate totaled $785/year. This was based on existing product/services in the market at the time EOBR II was drafted (February 2011). However, as noted above, the telematics industry responded heartily to the DOT's EOBR/HOS rulemaking (especially given the large market opportunity) and market competition has significantly driven costs down. For example, XRS (formerly XATA) markets its EOBR/HOS solution at $0 capital cost and $35/truck/month operating cost. In fact, the market response has been so strong that DOT intends to revise its EOBR cost projection substantially downward in the forthcoming update to its EOBR rules, which are anticipated by late 2013. The project team expects that DOT will estimate EOBR capital costs at well below $500/unit.

The ultimate cost of a Security EOBR will be determined by telematics service providers and competition in the market.

Product/service investment willingness by telematics service providers. The project team expects that telematics service providers will build EOBRs that Tier 1 HSSMs will

ESTIMATE OF THE NUMBER OF TIER 1 HSSM TELEMATICS UNITS REQUIRED.

	Estimated Number of "Security EOBR" Telematics Units Required	Estimated Number of Trailer Telematics Units Required
Straight Trucks	1,750	N.A.
Tractor/Trailers	5,000	12,500
Less Trailer Units Deployed	-	1,875
Estimated Units Required	6,750	10,625

Figure D-2.

> deploy. And like DOT, TSA will publish functional requirements that telematics service providers will use to refine their existing products/services to meet TSA's needs. In meetings with U.S. telematics service providers, the project team found that TSA's Security Action Items have had almost no impact on R&D decisions by telematics service providers, and scant impact on carrier telematics investment decision-making. Telematics service providers have not factored in TSA's Security Action Items into product planning and R&D investment, and do not plan to do so. In their view, government agencies are serious about their mission when they move forward with regulations, not voluntary measures like the SAIs. In addition, there has been little demand from the telematics service providers' carrier customers for enhanced security functionality in truck telematics systems. The foremost question on the minds of telematics service providers during project team site visits was market size. Will TSA programs create demand for telematics sales? How big is the opportunity?
>
> **Size of the market.** Telematics service providers will price products/services based, in part, on return on their R&D investment. They will set product/service prices based on the market size and their cost to serve that market. At a minimum, telematics service providers have to recover investment costs and minimal profit. Unlike the DOT EOBR market, though, the Tier 1 HSSM security market is small and, as yet, does not have a regulatory driver behind it.

Given the uncertainty introduced by telematics service provider pricing, the project team sought to establish a range of costs for tractor-based telematics systems (i.e. the Security EOBR) that it could use in its cost analysis. According to Frost & Sullivan, the pricing for a tractor-based telematics system is based on the hardware/software functionality built into it as well as the level of back-end data services required by a carrier.

As illustrated in **Figure D-3**, Frost & Sullivan estimates that a basic, stand-alone EOBR will cost up to $350. Monthly service charges will range from $20 to $30.

An EOBR that meets both DOT and TSA's needs, would, however, require enhanced hardware/software functionality. But, given the uncertainty over downstream pricing decision-making by Telematics service providers, the project team is unable to definitively establish a unit cost price point for the enhanced EOBR. Ultimately, that decision will lie in the hands of the Telematics service providers that choose to serve the Tier 1 HSSM market.

However, the project team estimates that TSP pricing would likely be about $750/unit, the upper end range for an entry level fleet management system that incorporates EOBR functionality.

But for purposes of its cost analyses, the project team will assume that the capital cost of an enhanced EOBR will be at least $500/tractor and cost, at most, $1,500/tractor, and will factor in a range of costs into its analyses.

It is also uncertain if the on-board computer in the DOT EOBR will need to be upgraded or replaced. So for purposes of this analysis, the project team assumed that all Tier 1 HSSM carriers will incur 100% EOBR replacement cost, a very conservative assumption. As illustrated in the **Figure D-4**, the capital cost to Tier 1 HSSM carriers would range from $3.38 million to $10.13 million.

The operating (service) cost for Tier 1 HSSM tractor-based Security EOBR telematics systems is estimated at $45/tractor/month, the high end of Frost & Sullivan's estimate for service costs for Mid-Level Fleet Management Systems. The project team elected to estimate tractor telematics operating costs at the high end because of the level of

COST OF TELEMATICS SYSTEMS.

	Track and Trace System	EOBR/Hours of Service	Entry Level Fleet Management System	Mid-Level Fleet Management System	High End Fleet Management System
	Collection of basic vehicle location data for tracking and back-end report generation	Stand-alone remote vehicle diagnostics + basic track & trace	EOBR plus basis FMS	Entry level plus navigation services and additional FMS applications	Mid-Level plus advanced vehicle/driver applications, advanced logistics management
Hardware Cost Range ($)	$200 - $300	$0 - $350	$500 - $750	$1,0000 - $1,500	$1,500 - $2,300
Service Cost Range ($ per tractor per month)	$10 - $20	$20 - $30	$25 - $35	$35 - $45	>$45

Figure D-3.

reporting TSA security requirements might impose on carriers, particularly as drive near or in High Threat Urban Areas. This generates an operating cost of $3,645,000/year for the entire Tier 1 HSSM fleet. A portion of operating costs of the Tier 1 fleet will be absorbed by DOT's EOBR requirements. Assuming an operating cost of $20/month/tractor for a DOT EOBR system, the net incremental operating cost for the Tier 1 HSSM fleet is $25/tractor/month or $2,025,000/year.

SECURITY EOBR CAPITAL COST FOR TIER 1 HSSM CARRIERS

Unit Cost to Replace EOBR Black Box	Total Cost to Replace EOBR Black Boxes for Tier 1 HSSM Carriers
$ 500 (Low Entry-Level FMS)	$ 3,375,000
$ 750 (High Entry-Level FMS)	$ 5,062,000 (most likely)
$ 1,000 (Low Mid-Level FMS)	$ 6,750,000
$ 1,500 (High Mid-Level FMS)	$ 10,125,000

Figure D-4.

For purposes of this estimate, Tier 1 HSSM carriers will incur the following capital and operating costs for tractor-based telematics.

- Capital cost range - $3,375,000 to $10,125,000
- Annual operating cost - $2,025,500/year (incremental over DOT EOBR operating cost)

Capital and Operating Cost – Trailer Telematics Units. According to Frost & Sullivan, there is a wide cost range for trailer/tanker telematics systems. TSA's trailer tracking needs will likely fall at the Mid-Level range as illustrated in **Figure D-5**.

For purposes of this analysis, the project team estimates that a Tier 1 HSSM carrier will incur capital unit costs of $550/trailer, the upper range of Frost & Sullivan's Mid-Level trailer telematics system costs. The project team estimates operating costs of $35/month/trailer, the highest monthly service cost reported by Frost & Sullivan, to account for potentially higher communications costs that TSA might require of Tier 1 HSSM carriers.

For the 10,625 Tier 1 HSSM trailers/tankers requiring telematics systems, the total estimated telematics cost will be:

- $5,843,750 capital cost; and
- $5,250,000 annual operating cost.

In Section V of this report, the project team presents its benefit/cost findings including a break-even analysis of the benefit/costs of a Tier 1 HSSM shipment tracking program. For purposes of that break-even analysis, the project team assumed that tractor telematics have a five year life, and trailer telematics have a ten year life.

Tier 1 HSSM Regulatory Compliance Costs

Tier 1 HSSM Shipper, Carrier, and Consignee Regulatory Compliance Costs. According to OMB guidance, costs incurred in an existing regulation should not be accounted for in a benefit/cost analysis of a new regulation. Most of the regulatory burden (compliance cost) that Tier 1 HSSM shippers and carriers might incur under a TSA HSSM security program have already been accounted for under existing DOT regulations. For example, DOT's HM-232 (49 CFR 172.800) requires shippers and carriers to develop and implement a written security plan for those who ship/transport certain hazardous materials. The DOT security plan must include the following:

- An assessment of transportation security risks for shipments of hazardous materials, including site-specific or location-specific risks associated with facilities at which the hazardous materials are prepared for transportation, stored, or unloaded incidental to movement and appropriate measures to address those risks
- Measures to confirm the information provided by job applicants who will have access to hazardous materials covered by the security plan

TRAILER TELEMATICS MARKET: PRODUCE AND SERVICE RANGE (NORTH AMERICA), 2010

	Entry Level	Mid-Level	High End
Hardware Cost Range ($)	$210 - $400	$400 - $550	$740 - $1400
Service Cost Range ($ per trailer per month)	$4.5 - $10	$10 - $20	$20 - $35

Figure D-5.

- Measures to prevent unauthorized access to hazardous material covered by the security plan, both on-site and during transport

The security plan, including the transportation security risk assessment, must be in writing and must be maintained for as long as it remains in effect. The security plan must be reviewed annually and revised and/or updated as necessary to reflect changing circumstances.

Hazardous materials employees at facilities where a security plan is required must receive in-depth training on parts of the security plan that they are responsible for. This training is required during their initial DOT training and at least every three years thereafter; or, if the security plan for which training is required is revised during the three-year recurrent training cycle, within 90 days of implementation of the revised plan. Regardless of whether a security plan is required, all hazardous materials employers are required to provide security awareness training to hazardous materials employees.

Another DOT regulatory requirement that will Tier 1 HSSM carriers must meet is the hazmat safety permit. A carrier must certify that it has a satisfactory security program, including:

(1) a security plan;

(2) a communications plan that allows for contact between the commercial motor vehicle operator and the motor carrier to meet the periodic contact requirements in § 385.415(c)(1); and

(3) successful completion by all hazmat employees of the security training required in § 172.704(a)(4) and (a)(5).

The carrier must also 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. The operator must make contact with the carrier at the beginning and end of each duty tour, and at the pickup and delivery of each permitted load. Contact may be by telephone, radio or via an electronic tracking or monitoring system. The motor carrier or driver must maintain a record of communications for 6 months after the initial acceptance of a shipment of hazardous material for which a safety permit is required. The record of communications must contain the name of the driver, identification of the vehicle, permitted material(s) being transported, and the date, location, and time of each contact required under this section.

In a cost/benefit assessment, TSA will only be responsible for the incremental regulatory burdens it places on Tier 1 HSSM shippers, carriers and consignees and the cost of those incremental regulatory burdens.

The project team developed an estimate of regulatory costs using current TSA Security Action Items as a surrogate for a TSA Tier 1 HSSM rule. As noted in **Figure D-6**, many of TSA's Security Action Items – if expressed as regulations – would already be covered by existing DOT rules or by other existing requirements (Security Action Items 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 16). Others are covered by telematics cost estimates (Security Action Items 21, 22, 23), or have no cost impact (Security Action Item 20).

Five Security Action Items will, however, have regulatory costs associated with them (Security Action Items 11, 12, 13, 17, 18). The estimated compliance costs associated with the Security Action Items are described in Figure E-6 and summarized below.

- SAI 11, Establish Appropriate Vehicle Security Program - $1,107,000 (one-time cost)

- SAI 12, Establish Cargo Security Program to Prevent Theft or Sabotage of Cargo Containers - $816,000 (one-time cost)

- SAI 13, Implement a Seal/Lock Control Program to Prevent Theft or Sabotage of Cargo - $2,600,000/year

- Security Action Item #17/#18. Shipment Pre-Planning, Advance Notice of Arrival and Receipt Confirmation Procedures with Receiving Facility - $4,000,000/year

Tier 1 HSSM Shipment Tracking Center Costs

The cost to build the Fedtrak R&D prototype into an operational Tier 1 HSSM shipment tracking center consistent with TSA's regulatory requirements and TSA's need for a tracking/risk system is estimated at $7 million. A shipment tracking center will provide 24/7 monitoring of all en-route Tier 1 HSSM shipments and will process Tier 1 HSSM electronic manifests and trip plans for Tier 1 HSSM shipments. Tracking center staff members are expected

ESTIMATED REGULATORY COMPLIANCE COSTS OF A TIER 1 HSSM PROGRAM.

TSA Security Action Item	Estimated Cost Impact
Security Action Item #1. Security Assessment and Security Plan Requirements (Tier 1 HSSM, Tier 2 HSSM)	Required under DOT security plan regulations.
Security Action Item #2. Awareness of Industry Security Practices (Tier 1 HSSM, Tier 2 HSSM)	Required under DOT security plan regulations.
Security Action Item #3. Inventory Control Process (Tier 1 HSSM, Tier 2 HSSM)	Already an established business practice for safety, security, and accounting purposes.
Security Action Item #4. Business and Security Critical Information (Tier 1 HSSM, Tier 2 HSSM)	Already an established business practice for safety, security, and accounting purposes.
Security Action Item #5. Possession of a Valid Commercial Driver's License -Hazardous Materials Endorsement (Tier 1 HSSM, Tier 2 HSSM)	Existing TSA requirement.
Security Action Item #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)	Existing TSA requirement.
Security Action Item #7. Security Awareness Training for Employees (Tier 1 HSSM, Tier 2 HSSM)	Existing requirement, but training of new employees will generate new costs. Already an established business practice for safety, security, and accounting purposes.
Security Action Item #8. Access Control System for Drivers (in addition to CDL) (Tier 1 HSSM, Tier 2 HSSM)	Required under DOT security plan rule.
Security Action Item #9. Access Control System for Facilities Incidental to Transport (Tier 1 HSSM, Tier 2 HSSM)	Already an established business practice for safety, security, and accounting purposes.
Security Action Item #10. Establish Communications Plan.	No significant cost. Assume all drivers have at least mobile phone.
Security Action Item #11. Establish Appropriate Vehicle Security Program. Other appropriate lockout control process.	TSA Trucking and Hazardous Materials Risk Assessment estimated a cost of $164/tractor for tractor secondary locks. Assuming 6,750 tractors, this SAI would have a one-time cost of $1,107,000.
Security Action Item #12. Establish Appropriate Cargo Security Program to Prevent Theft or Sabotage of Cargo Containers.	TSA Trucking and Hazardous Materials Risk Assessment estimated a cost of $96/trailer. Assuming 8,500 trailers, this SAI would have a one-time cost of $816,000.
Security Action Item #13. Implement a Seal/Lock Control Program to Prevent Theft or Sabotage of Cargo.	TSA Trucking and Hazardous Materials Risk Assessment estimated a cost of $1.30 per Tier 1 HSSM shipment. Assuming 2 million shipments, this SAI has a cost of $2,600,000/year.
Security Action Item #14. High Alert Level Protocols.	
	Required under DOT security plan rule.
Security Action Item #15. Establish Security Inspection Policy and Procedures.	Required under DOT security plan rule.
Security Action Item #16. Establish Reporting Policy and Procedures.	Required under DOT security plan rule.
Security Action Item #17. Shipment Pre-Planning, Advance Notice of Arrival and Receipt Confirmation Procedures with Receiving Facility	DOT estimates carriers will incur a cost of $2/trip to prepare a route plan. Preparation of shipping papers is already a requirement for carriers, so arguably there are no incremental costs associated with the preparation of electronic manifests by carriers. Given 2 million Tier 1 HSSM shipments/year, the cost of route plan preparation is $4million/year. The cost of processing electronic manifests and electronic trip plans are captured by the estimated cost of PSRC operation.

ESTIMATED REGULATORY COMPLIANCE COSTS OF A TIER 1 HSSM PROGRAM.	
Security Action Item #18. Preplanning Routes	Required under DOT security plan rule. See Security Action Item #17.
Security Action Item #19. Security for Trips Exceeding Driving Time under the Hours of Service of Drivers Regulation (49 CFR Part 395)	It is unlikely that TSA would adopt a regulatory requirement that Tier 1 HSSM trips that exceed DOT hours of service would require a two-person driver team. More likely, this would be a rule that falls under DOT's Hours of Service program, and costs associated with a 2-driver rule would be accounted for as a safety benefit in the DOT rulemaking. Development of a safe haven rule under consideration in DOT may also substantially change the regulatory landscape as might telematics tradeoffs that might potentially eliminate or minimize the need for 2-driver teams.
Security Action Item #20. Dedicated Truck	According to TSA's Trucking and Hazardous Materials Risk Assessment, this is not a cost item. Also, an electronic manifest program – priced out under centralized shipment tracking center operating cost calculations – would reinforce business practices that would discourage transloading and driver/team substitutions.
Security Action Item #21. Tractor Activation Capability	Accounted for under tractor telematics cost.
Security Action Item #22. Panic Button Capability	Accounted for under tractor telematics cost.
Security Action Item #23. Tractor and Trailer Tracking Systems	Accounted for under tractor telematics cost.

Figure D-6.

to support a robust service function for tracking center customers and maintain/update operating and database systems. The systems that support those functions are included in the development estimate above. In addition, tracking center staff will establish and maintain system connections with Federal and State partners.

The cost to operate the tracking center will have fixed and variable components, and for purposes of this estimate the project team estimates tracking center fixed costs at $7million/year. Tracking center variable costs will be a function of the number of transactions processed through the tracking center and the number of shipments monitored by tracking center Security Specialists. The project team believes that the USPS Priority Mail Flat Rate Envelope rate of $5.60 is a reasonable surrogate for PSRC electronic manifest/trip plan transactional costs. Assuming 2 million Tier 1 HSSM shipments per year, tracking center variable costs are estimated at $11.2 million/year. Thus, total tracking center annual operating costs are estimated at $18.2 million/year ($7 million fixed and $11.2 million variable). Note that tracking center operating cost may be borne partially or fully by Tier 1 HSSM trading partners (shippers, carriers, consignees).

Summary: Tier 1 HSSM Program Costs

Figure D-7 summarizes the project team's estimated costs associated with a Tier 1 HSSM shipment tracking program.

Figure D-8 illustrates the estimated cost of TSA's Tier 1 HSSM program over time. The following assumptions were made in compiling Figure E-8:

- tractors/straight trucks have a 5 year life. Telematics are replaced every 5 years;
- trailers have a 10 year life. Telematics are replaced every 10 years;
- inflation = discount rate; and
- security benefit = $5.3 Billion.

SUMMARY OF ESTIMATED COST OF A TIER 1 HSSM SHIPMENT TRACKING PROGRAM

Cost Category		**Estimated Costs**			
Telematics Capital & Operating Cost – Tier 1 HSSM Carriers	Security EOBR 5,000 tractors 1,750 straight trucks	Capital Cost Range/Unit	$ 500 (low Entry Level FMS)	$ 3,375,000	
			$ 750 (high Entry Level FMS)	**$ 5,062,000 (most likely)**	
			$ 1,000 (low Mid-Level FMS)	$ 6,750,000	
			$ 1,500 (high Mid-Level FMS)	$ 10,125,000	
		Operating Cost	Monthly	Total - Annual	
			$25/unit (net)	$2,025,500	
	Trailer Telematics 10,625 trailers/ tankers	Capital Cost	Per Unit	Capital Cost – Total	
			$550	$5,843,750	
		Operating Cost	Monthly	Total - Annual	
			$35/unit	$5,250,000	
Tier 1 HSSM Regulatory Compliance Cost		One-Time Cost		$1,923,000	
		Annual Cost		$6,600,000	
Tier 1 HSSM Shipment Tracking Center		Cost to Place Into Operation		$7,000,000	
		Annual Operating Cost		Fixed Cost Component	$7,000,000
				Variable Cost Component	$11,200,000

Figure D-7.

COST OF TIER 1 HSSM PROGRAM OVER TIME

Year	Telematics Capital Cost (Tractor)	Telematics Operating Cost (Tractor)	Telematics Capital Cost (Trailer)	Telematics Operating Cost (Trailer)	Tracking Center Operations	Regulatory Compliance Cost	Cumulative Cost	Benefit/Cost Ratio
0					$7,000,000	$1,923,000	$8,923,000	
1	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$51,904,250	102.11
2		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$83,979,750	63.11
3		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$116,055,250	45.67
4		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$148,130,750	35.78
5		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$180,206,250	29.41
6	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$217,343,750	24.39
7		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$249,419,250	21.25
8		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$281,494,750	18.83
9		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$313,570,250	16.90
10		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$345,645,750	15.33
11	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$388,627,000	13.64
12		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$420,702,500	12.60
13		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$452,778,000	11.71
14		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$484,853,500	10.93
15		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$516,929,000	10.25
16	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$554,066,500	9.57
17		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$586,142,000	9.04
18		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$618,217,500	8.57
19		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$650,293,000	8.15
20		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$682,368,500	7.77
21	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$725,349,750	7.31
22		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$757,425,250	7.00
23		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$789,500,750	6.71
24		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$821,576,250	6.45
25		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$853,651,750	6.21
26	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$890,789,250	5.95
27		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$922,864,750	5.74
28		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$954,940,250	5.55
29		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$987,015,750	5.37
30		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,019,091,250	5.20
31	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$1,062,072,500	4.99
32		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,094,148,000	4.84
33		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,126,223,500	4.71
34		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,158,299,000	4.58
35		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,190,374,500	4.45
36	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,227,512,000	4.32
37		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,259,587,500	4.21
38		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,291,663,000	4.10

COST OF TIER 1 HSSM PROGRAM OVER TIME

39		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,323,738,500	4.00
40		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,355,814,000	3.91
41	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$1,398,795,250	3.79
42		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,430,870,750	3.70
43		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,462,946,250	3.62
44		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,495,021,750	3.55
45		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,527,097,250	3.47
46	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,564,234,750	3.39
47		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,596,310,250	3.32
48		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,628,385,750	3.25
49		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,660,461,250	3.19
50		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,692,536,750	3.13
51	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$1,735,518,000	3.05
52		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,767,593,500	3.00
53		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,799,669,000	2.94
54		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,831,744,500	2.89
55		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,863,820,000	2.84
56	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,900,957,500	2.79
57		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,933,033,000	2.74
58		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,965,108,500	2.70
59		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$1,997,184,000	2.65
60		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,029,259,500	2.61
61	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$2,072,240,750	2.56
62		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,104,316,250	2.52
63		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,136,391,750	2.48
64		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,168,467,250	2.44
65		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,200,542,750	2.41
66	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,237,680,250	2.37
67		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,269,755,750	2.34
68		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,301,831,250	2.30
69		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,333,906,750	2.27
70		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,365,982,250	2.24
71	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$2,408,963,500	2.20
72		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,441,039,000	2.17
73		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,473,114,500	2.14
74		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,505,190,000	2.12
75		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,537,265,500	2.09
76	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,574,403,000	2.06
77		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,606,478,500	2.03
78		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,638,554,000	2.01
79		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,670,629,500	1.98
80		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,702,705,000	1.96

COST OF TIER 1 HSSM PROGRAM OVER TIME

81	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$2,745,686,250	1.93
82		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,777,761,750	1.91
83		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,809,837,250	1.89
84		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,841,912,750	1.86
85		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,873,988,250	1.84
86	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,911,125,750	1.82
87		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,943,201,250	1.80
88		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$2,975,276,750	1.78
89		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,007,352,250	1.76
90		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,039,427,750	1.74
91	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$3,082,409,000	1.72
92		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,114,484,500	1.70
93		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,146,560,000	1.68
94		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,178,635,500	1.67
95		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,210,711,000	1.65
96	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,247,848,500	1.63
97		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,279,924,000	1.62
98		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,311,999,500	1.60
99		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,344,075,000	1.58
100		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,376,150,500	1.57
101	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$3,419,131,750	1.55
102		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,451,207,250	1.54
103		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,483,282,750	1.52
104		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,515,358,250	1.51
105		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,547,433,750	1.49
106	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,584,571,250	1.48
107		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,616,646,750	1.47
108		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,648,722,250	1.45
109		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,680,797,750	1.44
110		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,712,873,250	1.43
111	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$3,755,854,500	1.41
112		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,787,930,000	1.40
113		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,820,005,500	1.39
114		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,852,081,000	1.38
115		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,884,156,500	1.36
116	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,921,294,000	1.35
117		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,953,369,500	1.34
118		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$3,985,445,000	1.33
119		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,017,520,500	1.32
120		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,049,596,000	1.31
121	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$4,092,577,250	1.30
122		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,124,652,750	1.28

COST OF TIER 1 HSSM PROGRAM OVER TIME

123		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,156,728,250	1.28
124		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,188,803,750	1.27
125		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,220,879,250	1.26
126	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,258,016,750	1.24
127		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,290,092,250	1.24
128		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,322,167,750	1.23
129		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,354,243,250	1.22
130		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,386,318,750	1.21
131	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$4,429,300,000	1.20
132		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,461,375,500	1.19
133		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,493,451,000	1.18
134		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,525,526,500	1.17
135		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,557,602,000	1.16
136	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,594,739,500	1.15
137		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,626,815,000	1.15
138		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,658,890,500	1.14
139		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,690,966,000	1.13
140		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,723,041,500	1.12
141	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$4,766,022,750	1.11
142		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,798,098,250	1.10
143		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,830,173,750	1.10
144		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,862,249,250	1.09
145		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,894,324,750	1.08
146	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,931,462,250	1.07
147		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,963,537,750	1.07
148		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$4,995,613,250	1.06
149		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,027,688,750	1.05
150	$5,062,000	$2,025,500	$5,843,750	$5,250,000	$18,200,000	$6,600,000	$5,070,670,000	1.05
151		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,102,745,500	1.04
152		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,134,821,000	1.03
153		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,166,896,500	1.03
154		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,198,972,000	1.02
155	$5,062,000	$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,236,109,500	1.01
156		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,268,185,000	1.01
157		$2,025,500		$5,250,000	$18,200,000	$6,600,000	$5,300,260,500	1.00

Figure D-8.

ANNEX E

Section 1554(a)(2)(c) Evaluation Summary

In Section VI, the project team presented its summary recommendations. This annex summarizes the project team's findings in relation to eight specific evaluation items in Section 1554(a)(2)(C).

> 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

FMCSA's 2004 Hazardous Materials Safety & Security Operational Field Test quantified the security benefits associated with the deployment of truck telematics systems. According to the FMCSA study, security benefits will exceed $5 Billion.

Annex C describes the methodology used by the FMCSA project team to quantify security benefits.

The security benefits findings from FMCSA's 2004 Hazardous Materials Safety & Security Operational Field Test are still valid and relevant to the Section 1554 benefit/cost analysis.

The security benefits methodology in FMCSA's Hazardous Materials Safety & Security Operational Field Test was sophisticated, comprehensive, and consistent with current DHS risk approaches. The FMCSA project team employed a sophisticated and comprehensive approach to quantifying benefits, especially security benefits. The methodology was based on the 'threat, vulnerability, consequence' risk approach in use today at DHS as well as specific threat scenarios that TSA has incorporated into its highway program. A large group of subject matter experts from industry and government fed their expertise into the Hazardous Materials Safety & Security Operational Field Test.

Explosives and bulk chemicals are Tier 1 HSSMs. The Hazardous Materials Safety & Security Operational Field Test was completed before TSA issued its list of Tier 1 HSSMs – the riskiest materials on the nation's roads. However, two groups of hazardous materials studied – explosives and bulk chemicals – are Tier 1 HSSMs. As "pure play" Tier 1 HSSMs, conclusions reached by the FMCSA project team in terms of benefits for these materials are applicable to TSA's present day highway hazmat security program.

Security benefits are likely understated. The Hazardous Materials Safety & Security Operational Field Test quantified security benefits using the standard DOT/DHS risk equation in which Risk (cost) = threat x vulnerability x consequence. In general, the security benefit is a function of the amount of vulnerability reduction that telematics systems offer for explosives shipments or bulk chemical shipments. Vulnerability reduction in the study is likely understated – perhaps significantly so – in relation the vulnerability reduction that TSA might capture with an enhanced "security" telematics package, tighter chain-of-custody control via an electronic manifest program, and closer shipment monitoring via centralized shipment tracking.

The security benefits associated with the deployment of truck telematics systems are in addition to the operational benefits that truck telematics systems offer hazmat carriers. According to the FMCSA study, deployment of truck telematics systems will generate $10,968/truck/year in operational savings for an explosives carrier and $7,116/year/truck for a bulk chemicals carriers (see **Figure V-1**).

The project team estimated the cost of deploying and operating tractor- and trailer-based telematics systems in the context of a concept of operations plan that requires Tier 1 HSSM carriers to deploy telematics equipment and report data to a shipment tracking center. **Section IV** describes the concept of operations plan developed by

TRUCK TELEMATICS AND SECURITY BENEFITS – TIER 1 HSSM SHIPMENTS

	Vulnerability Reduction %		Security Benefit (in Millions of Dollars)	
Telematics Technology Package	Bulk Chemicals	Truckload Explosives	Bulk Chemicals	Truckload Explosives
WC + GPS Position	16%	12%	$2,581	$1,657
WC + GPS Position + Panic Alert	25%	21%	$4,058	$2,822
WC + GPS Position + PSRC	24%	20%	$3,891	$2,652
WC + GPS Position + Vehicle Disabling + Panic Alert	31%	**25%**	**$5,098**	$3,355
WC + GPS Position + Panic Alert + Driver ID + ESCM	33%	**26%**	**$5,319**	**$3,510**

Figure V-2.

the project team. In estimating costs, the project team had to answer the following questions.

- How many Tier 1 HSSM shipments are there annually?
- What is the unit capital cost for tractor- and trailer-based telematics systems?
- What is the annual operating cost of tractor- and trailer-based telematics systems?
- How many tractors or straight trucks need to be equipped with telematics equipment?
- How many trailers need to be equipped with telematics equipment?
- What is the compliance cost of a Tier 1 HSSM regulatory program?
- What is the cost of establishing and operating a shipment tracking center?

The project team compiled costs in three categories: 1) telematics capital and operating costs; 2) compliance costs; and 3) centralized shipment tracking costs. **Figure D-8** presents the estimated cost of TSA's Tier 1 HSSM program over time. The cost assumptions/findings of the project team are described more fully in **Annex D**.

A key recommendation of the project team is that TSA leverage DOT's EOBR initiative by enhancing the basic telematics functionality in DOT's EOBR so that it can operate as a combined safety and security EOBR for deployment by Tier 1 HSSM carriers. This **Security EOBR** would not only have the functionality to meet DOT's Hours of Service needs, but would include extra functionality to meet TSA's security needs for Tier 1 HSSM carriers.

Section III presents the functional requirements for the Security EOBR. **Figure III-7** presents a summary of the functional requirements.

Using DOT's EOBR as a foundational telematics platform offers TSA and the carrier community a number of advantages.

Consistency with Section 1554 collaboration mandate. Section 1554 requires TSA to consult with DOT as it develops its shipment tracking program. Development of the Security EOBR will bring TSA and DOT telematics initiatives into close alignment, meeting the spirit and intent of Section 1554.

Shared data/performance standards. DOT has done a great deal of work in defining data standards and in developing performance standards for its EOBR/Hours of Service program. By leveraging this work, TSA can not only achieve programmatic consistency but also substantially reduce its burden in developing its security telematics solution. Tier 1 HSSM carriers – jointly regulated by DOT (safety) and TSA (security) – will also benefit from a single, comprehensive set of data and performance standards.

Simpler telematics solution; leverage investment by telematics service providers. The Security EOBR will satisfy a Tier 1 HSSM carrier's Hours of Service (safety) and security requirements with a single telematics unit instead of separate safety and security devices, lowering capital costs. Also, carrier operating costs, especially communications costs, will be lower in a combined telematics solution. Telematics service providers can leverage existing EOBR/HOS software investment by integrating safety and security applications in a combined EOBR.

An EOBR that meets both DOT and TSA's needs would, however, require enhanced hardware/software functionality. But, given the uncertainty over downstream pricing decision-making by telematics service providers, the project team was unable to definitively establish a unit cost price point for the enhanced EOBR. However, the project team's best estimate of the unit cost of a Security EOBR is about $750/unit. Refer to **Annex D** for additional discussion.

Section V presents the project team's benefit/cost findings. Benefit/cost analyses support a strongly compelling argument that TSA should move forward with a Tier 1 HSSM shipment tracking program that requires deployment of truck telematics systems by Tier 1 HSSM carriers, implementation of an electronic manifest system, and reporting to a Public Sector Reporting Center.

A breakeven analysis of security benefits and costs indicate that a Tier 1 HSSM shipment tracking program is warranted if it prevents a single terrorist attack in the next 157 years. Security benefits outweigh costs by 46:1 using the 3-year timeframe for evaluating benefits and costs adopted in FMCSA's Hazardous Materials Safety & Security Operational Field Test. Security benefits outweigh costs by 15:1 using a more conservative 10-year timeframe. Normally, a benefit/cost ratio greater than 1:1 is sufficient justification for a Federal agency to move forward with a regulatory program.

ii THE ABILITY OF TRACKING TECHNOLOGY TO RESIST TAMPERING AND DISABLING

There are two ways to disable tractor-based or trailer/tanker-based telematics systems: 1) physically disabling the system by tampering with wiring and/or telematics hardware; or 2) remotely disabling/blocking the GPS and or GSM functionality of the telematics system using non-physical means.

The U.S. telematics industry is lagging behind other countries when it comes to security innovations. Telematics systems offered by telematics service providers in other countries have been "hardened" to resist physical attacks. Also, "anti-jamming" GPS chips are offered in tractor-based telematics systems that are programmed to detect and warn against GPS and GSM jamming attacks.

Section III presents the project team's findings related to tampering and disabling of telematics systems. The project team made five recommendations.

1. Telematics hardware – including cables, wires, terminals, antennas, black boxes – must be secured against attempts to defeat them by physical means, both on the tractor as well as trailers/tankers. TSA should adopt regulations/standards – at least as stringent as those for high value goods shipments – for the physical security of truck/trailer-based telematics systems.

2. TSA should adopt requirements for covert installation of telematics hardware at least as stringent as TAPA's Trucking Security Requirements (TSR) for high value goods shipments. TSA should adopt a requirement for trailer door and tanker hatch locks at least as stringent as TAPA's Trucking Security Requirements (TSR) for high value goods shipments.

3. The tractor-based Security EOBR must detect and report trailer/tanker untethering (disconnects) between gate-out and gate-in. TSA should leverage the DOT EOBR hardware tampering requirements. TSA should add a sensor to report trailer/tanker untethering (disconnect) to tractor-based EOBR between gate-out and gate-in.

4. Trailer-based telematics system must detect and report trailer door opening and open/close door status. Tanker-based telematics system must detect and report hatch opening and open/close hatch status. Add the following reportable events (time and location stamped): 1) trailer door open/close; 2) trailer door status; 3) hatch open/close; and 4) hatch status.

5. The Security EOBR must detect a GSM/GPS jamming attack and send an alert message to the PSRC, the carrier, and to the driver. This means the Security EOBR must incorporate GPS chip/software to detect a jamming attack and a hybrid satellite/cellular modem to send a message to the PSRC (and to continue location reporting) even if the cellular network has been compromised by jamming.

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

FMCSA's 2004 Hazardous Materials Safety & Security Operational Field Test first advanced the concept of the Public Sector Reporting Center, a centralized tracking/monitoring facility for shipments of hazardous materials.

Development of a Public Sector Reporting Center concept of operations plan was not the main focus of the FMCSA study, and FMCSA recommended that a follow-on study assess the feasibility of implementing a Public Sector Reporting Center for hazmat shipments. Based on FMCSA's recommendation, Congress directed TSA to conduct the Hazmat Truck Security Pilot (2007) to determine if a Public Sector Reporting Center was feasible. A technology prototype of a hazmat shipment tracking system was built and operated on a limited basis. The study proved that development of a Public Sector Reporting Center was technically feasible. However, the technology prototype fell far short of an operational shipment tracking system for Tier 1 HSSMs. Also, the Pilot did not examine many of the technology, cost, and programmatic issues that would be important in implementing a national shipment tracking system for Tier 1 HSSMs.

TSA's Fedtrak R&D initiative picked up where the Hazmat Truck Security Pilot left off with the aim of building the software and systems needed to support an operational Tier 1 HSSM shipment tracking program. The Fedtrak project team conducted a detailed gap analysis of the Hazmat Truck Security Pilot technology prototype and used that gap analysis, in part, to construct an architectural plan for an operational Tier 1 HSSM shipment tracking system. The team also completed an analysis of TSA's future operating requirements, including those related to Section 1554, and constructed a set of requirements for TSA's Public Sector Reporting Center.

Section IV describes how a Public Sector Reporting Center will work in the context of a concept of operations plan for TSA's Tier 1 HSSM shipment tracking program. TSA's Tier 1 HSSM Public Sector Reporting Center needs to serve a variety of functions including the following:

- 24/7/365 real-time tracking platform for Tier 1 HSSM shipments that provides TSA visibility into the movement of Tier 1 HSSM shipments over the nation's road system;
- risk management platform that identifies the riskiest en-route shipments on a real-time basis and allows TSA to proactively manage risk in the hazmat supply chain;
- implementing tool for a TSA Tier 1 HSSM regulatory program focused on supply chain risk reduction;
- tool for Tier 1 HSSM shippers, carriers and consignees that have Tier 1 HSSM regulatory compliance responsibilities;
- electronic manifest and routing solution for Tier 1 HSSM shipments (chain-of-custody and route adherence monitoring);
- collaboration platform to manage Tier 1 HSSM security incidents by bringing together federal, state, and local response agencies as well as HSSM trading partners (shippers, carriers, and consignees) in the resolution of the incident; and
- extensive warehouse of data on Tier 1 HSSM transactions/shipments over U.S. roads.

Section III presents a set of requirements and a high-level architectural plan for a Public Sector Reporting Center developed as part of the Fedtrak research and development initiative (**Figure IV-1**).

iv THE APPROPRIATE RANGE OF CONTACT INTERVALS BETWEEN THE TRACKING TECHNOLOGY AND A COMMERCIAL MOTOR VEHICLE TRANSPORTING SECURITY-SENSITIVE MATERIALS

In **Section III**, the project team presents recommendations in regards to contact intervals and TSA's highway hazmat security program.

The shipment tracking center needs to be able to "interrogate" a Security EOBR at any time on a machine-to-machine (M2M) basis to determine the real-time location of a shipment of Tier 1 HSSMs. This means that security personnel at the tracking center must be able to "ping" the Security EOBR installed on a tractor at any time to get its location.

Figure III-2 lists events that a Security EOBR should automatically report to the shipment tracking center as the event occurs. An event report will include an event code, the telematics unit identification number, the location where the event occurred (latitude/longitude), and time the event occurred.

Security EOBRs will report events as they occur, however, location reporting rates will vary depending on the tractor's location and its security status. In general, the triggers for variable reporting are as follows.

- A security incident will require increased location reporting
- Travel in or close to a High Threat Urban Area will require increased location reporting.
- Travel in a cellular dark zone will require location reporting via a satellite network, but at a reduced reporting rate.

For Tier 1 HSSM shipments traveling through TSA-designated High Threat Urban Areas (HTUAs), the Security EOBRs should be programmed to report location to the shipment tracking center once/minute, the same location reporting standard used by the Singapore Civil Defence Force for trucks traveling on Singaporean roads. Location reporting will increase to every fifteen seconds in the event of a security incident. Note that cellular networks will be readily available in the HTUAs – thus making it a rare event that reporting will need to be made over the more costly, backup satellite system. **Figure III-3** summarizes the project team's recommendations for Security EOBR tractor location reporting.

Two-way (M2M) messaging between the Security EOBR and the shipment tracing center is needed to support vehicle disabling, location polling, variable location reporting, and event reporting. The Universal Communications Interface (UCI) developed during TSA's Hazmat Truck Security Pilot was built assuming there would be only one-way messaging – from a telematics service provider to the shipment tracking center. Two-way, machine-to-machine (M2M) messaging between the tracking center and the Security EOBR is needed to provide TSA the security functionality it needs, especially in terms of managing reporting frequency and in managing communications during a security incident. For example, TSA will require more frequent location reporting for a shipment in a High Threat Urban Area than a shipment well outside the HTUA. The UCI will need to be re-engineered to support M2M messaging. Also, tracking center systems may direct the Security EOBR on a tractor to increase location reporting if the shipment is off route.

Trailers and tankers will have telematics systems separate from tractor-based systems, and different location/event reporting requirements. In general, a heavier reporting burden will be placed on the Security EOBR than trailer/tanker-based systems. Trailer/tanker-based systems are usually battery-powered, unlike tractor-based systems, and battery life preservation is important. Also, location reporting from trailers/tankers is less important when they are paired with a tractor. Location reporting becomes important when a trailer or tanker is unexpectedly disconnected from a tractor between gate-out and gate-in, indicating the possible theft or diversion of HSSMs. **Figure III-4** lists events that a tractor-based telematics system should automatically report to the shipment tracking center.

Figure III-5 summarizes the project team's recommendations for trailer/tanker location reporting frequency. Note that the project team expects almost all location reporting will take place over cellular networks.

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

Section III presents the project team's recommendations for vehicle disabling.

1. The Security EOBR should have the capability to allow a carrier to remotely disable a tractor hauling Tier 1 HSSMs upon direction by TSA and/or authorized state or local law enforcement agency.
2. A Tier 1 HSSM driver should not be able to start or drive a truck hauling HSSMs without authenticating his/her identity using the Security EOBR.
3. The Security EOBR should have the capability to automatically disable a tractor when that tractor enters a No Drive Zone established by TSA.
4. The Security EOBR should have the capability to allow TSA and/or an authorized state/local law enforcement agency to remotely disable a tractor hauling Tier 1 HSSMs. The Security EOBR should be able to accept a disabling message – from the carrier, law enforcement agency, or TSA – via cellular and satellite networks.

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

viii OTHER SYSTEMS AND INFORMATION THE SECRETARY DETERMINES APPROPRIATE

In developing a tracking program for security-sensitive materials as called for under Section 1554 of the 9/11 Act, TSA should issue regulations that require Tier 1 highway security sensitive materials (HSSM) carriers to deploy telematics systems and report data to a Public Sector Reporting Center.

DOT's EOBR experience shows that carriers will not deploy telematics systems without a regulatory driver. Also, telematics service providers will be reluctant to invest research and development funds into product/service refinement without the certainty of government regulations and specific functional requirements.

A regulatory program that requires Tier 1 HSSM carriers to deploy truck telematics systems and report data to a shipment tracking center will significantly reduce risk in the hazmat supply chain. The security benefit of this reduced risk is estimated at $5.3 billion for Tier 1 shipments according to FMCSA's Hazardous Materials Safety & Security Operational Field Test.

Benefit/cost analyses support a strongly compelling argument that TSA should move forward with a Tier 1 HSSM regulatory program. A breakeven analysis of security benefits and costs indicate that a Tier 1 HSSM shipment tracking program is warranted if it prevents a single terrorist attack in the next 157 years. Security benefits outweigh costs by 46:1 using the 3-year timeframe for evaluating benefits and costs presented in FMCSA's Hazardous Materials Safety & Security Operational Field Test. Security benefits outweigh costs by 15:1 using a more conservative 10-year timeframe. Normally, a benefit/cost ratio greater than 1:1 is sufficient justification for a Federal agency to move forward with a regulatory program.

The project team recommends that TSA leverage DOT's EOBR initiative by enhancing the basic telematics functionality in DOT's EOBR so that it can operate as a combined safety and security EOBR for deployment by Tier 1 HSSM carriers. This **Security EOBR** would not only have the functionality to meet DOT's Hours of Service needs, but would include extra functionality to meet TSA's security needs. **Section III** describes the functional requirements for the Security EOBR. **Figure III-7** presents a summary of the functional requirements.

• • •

ABBREVIATIONS AND ACRONYMS

ACE	CBP Automated Commercial Environment Truck E-Manifest
ANPRN	Advanced Notice of Proposed Rulemaking
CBP	United States Customs and Border Protection
DTTS	DOD Defense Transportation Tracking System
DHS	United States Department of Homeland Security
DOD	United States Department of Defense
DOT	United States Department of Transportation
E-LOCK	Electronic Cargo (Door/Hatch) Lock
E-MANIFEST	Electronic Manifest
E-ROUTE PLAN	Electronic Route Plan
EOBR	Electronic On Board Recorder
FMCSA	United State Federal Motor Carrier Safety Administration
FOT	FMCA's Hazardous Materials Safety & Security Operational Field Test
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSPD	Homeland Security Presidential Directive
HSSM	Highway Security Sensitive Material
HTSP	TSA's Hazmat Truck Security Pilot
KTC	Kentucky Transportation Center, University Of Kentucky
MAP-21	Moving Ahead For Progress In The 21st Century Act
M2M	Machine To Machine
NPRN	Notice of Proposed Rulemaking
PSRC	Public Sector Reporting Center
ROI	Return On Investment
SAI	TSA Security Action Item
SCDF	Singapore Civil Defence Force
TAPA	Transported Asset Protection Association
TIER 1 HSSM	Tier 1 Highway Security Sensitive Material
TRANSCOM	DOE Transportation Tracking and Communications System
TSA	United States Transportation Security Administration
TSP	Telematics Service Provider
1554	Section 1554 of the 9/11 Act of 2007