Excellence In Motion

The North American Transportation Security Center -- Technology Prototype Gap Analysis

Report Number: KTC-19-31/FD03-1F

DOI: https://doi.org/10.13023/ktc.rr.2019.31

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

in cooperation with
Kentucky Transportation Cabinet
Commonwealth of Kentucky

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

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

in cooperation with
Kentucky Transportation Cabinet
Commonwealth of Kentucky

KTC KENTUCKY
Transporation Center

Kentucky Transportation Center • University of Kentucky
176 Raymond Building • Lexington, KY 40506 • 859.257.6898 • www.ktc.uky.edu

UK University of
Kentucky

Research Report
KTC-19-31/FD03-1F

The North American Transportation Security Center – Technology Prototype Gap Analysis

Doug Kreis, Ph.D., PE
Associate Director

and

Michael Barclay
Coldstream Digital

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

In Cooperation With
Kentucky Transportation Cabinet
Commonwealth of Kentucky

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

May 2009

Executive Summary

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

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

The FMCSA study led to the **U.S. Transportation Security Administration's** (TSA) Hazmat Truck Security Pilot (HTSP). This congressionally mandated pilot program was undertaken to demonstrate if a hazmat truck tracking center was feasible from a technology and systems perspective. The HTSP project team built a technology prototype of a hazmat truck tracking system to show that "smart truck" technology could be crafted into an effective and efficient system for tracking hazmat shipments. The HTSP project team also built the Universal Communications Interface – the XML gateway for hazmat carriers to use to provide data to a centralized truck tracking center.

In August 2007, Congress enacted the 9/11 Act (PL110-53) that directs TSA to develop a program - consistent with the Hazmat Truck Security Pilot - to facilitate the tracking of motor carrier shipments of security-sensitive materials. In June 2008, TSA took a major step forward in establishing a national hazmat security program by issuing guidance for shipments of Tier 1 Highway Security Sensitive Materials (HSSMs), the riskiest shipments from a security perspective. TSA's Tier 1 HSSM guidance includes Security Action Items which specify security measures – including vehicle tracking – that TSA believes are prudent security measures for shippers and carriers to follow. Compliance with TSA's Tier 1 HSSM guidance is voluntary but TSA is expected to issue regulations based on the Tier 1 HSSM Security Action Items that will make compliance mandatory.

Establishment of a Tier 1 HSSM truck tracking center is critical to implementation of a Tier 1 HSSM regulatory program based on the Security Action items by TSA. The HTSP technology prototype was an excellent first step toward an operational Tier 1 HSSM truck tracking system, however, it falls far short of what TSA needs in an operational system.

This deliverable examines the "gaps" between the HTSP technology prototype and an operational Tier 1 HSSM truck tracking system. It draws upon the work of an Independent Verification and Validation contractor that evaluated the HTSP technology prototype. It also examines TSA needs related to implementation of a regulatory program based on Tier 1 HSSM Security Action Items.

blank page

Table of Contents

blank

1.0 The TSA Hazmat Truck Security Pilot Technology Prototype

After the FMCSA finished its Hazmat Safety and Security Technology Field Operational Test (FOT) in November 2004, Congress directed the **U.S. Transportation Security Administration** (TSA) to undertake the TSA Hazmat Truck Security Pilot (HTSP) project. The purpose of the pilot project was to demonstrate that a hazmat truck tracking center was feasible from a technology and systems perspective and to determine if existing commercial truck tracking systems can interface with government intelligence centers and first responders.

The contract for the Hazmat Truck Security Pilot program was awarded to **General Dynamics Advanced Information Systems** (GDAIS) of Buffalo, NY in October 2005. Work under the contract was completed April 2008. The contract had three tasks.

1. Develop and demonstrate a prototype for a centralized truck tracking center that could be used to continually track truck locations and load types. The truck tracking center would also be used to coordinate incident response with a government intelligence operations center, state, local, and Federal law enforcement agencies and first responders.
2. Develop and demonstrate a non-proprietary universal interface or set of communication protocols that would allow alerts and tracking information to be transmitted from all commercially available tracking systems to a prototype truck tracking center.
3. Analyze the feasibility and benefits of applying a risk-based approach to identifying and managing hazmat security risks and incidents involving trucks on U.S. highways; demonstrate the capability of using the Hazmat Truck Security System (HTSS), with a commercial-off-the-shelf (COTS) rules-based risk assessment tool; and conduct a public showcase demonstration of the entire HTSS.

The Hazmat Truck Security Pilot (HTSP) program demonstrated that a truck tracking system is feasible from a technology and systems perspective.

Congress directed TSA to undertake the Hazmat Truck Security Pilot project. TSA demonstrated that a truck tracking system is feasible from a technology and systems perspective.

1.1 What are the building blocks of a hazmat truck tracking center?

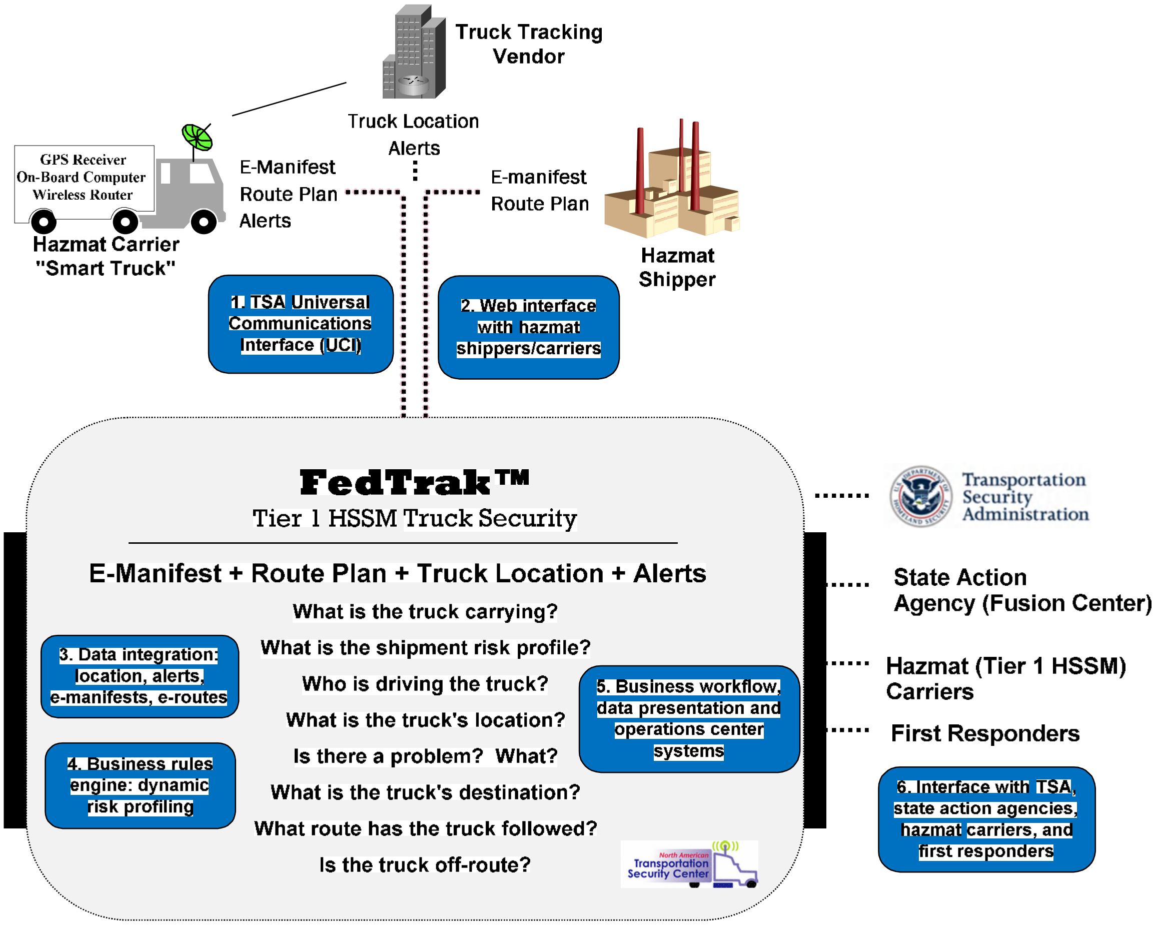
Figure 1.1 presents a general schematic of a hazmat truck tracking center. As indicated in Figure 1.1, six basic functional components – or building blocks - are needed to build a hazmat truck tracking system.

1. An **XML-based interface** with fleet tracking vendors feeds data to a hazmat truck tracking center.
2. A **web interface** (portal) allows shippers and carriers to interact with the truck tracking center (registration, e-manifest, e-route) and to submit/view corporate data.
3. The hazmat truck tracking operations center **merges data** flowing into it to create actionable information for government agencies.
4. A **risk (business rules) engine** provides dynamic risk profiling of hazmat shipments between gate-out and gate-in to identify "risky" shipments..
5. Business **process workflow processing and data processing** results are displayed on desktops and workstations in a truck tracking operations center.
6. A **communications infrastructure** supports efficient interaction/consultation with government action agencies, hazmat carriers, and first responders.

The building blocks of a hazmat truck tracking center are:

1. an XML –based communications interface;
2. a portal interface for hazmat shippers and carriers
3. an operations center that processes data into actionable intelligence;
4. a business rules engine for dynamic risk profiling of hazmat shipments;
5. systems to manage business workflow and data presentation; and
6. a communications infrastructure to support collaboration with government action agencies and others.

Figure 1.1 Building blocks of a hazmat truck tracking center.


Truck Tracking Vendor
Truck Location Alerts
GPS Receiver
On-Board Computer
Wireless Router
Hazmat Carrier "Smart Truck"
E-Manifest
Route Plan
Alerts
E-manifest
Route Plan
Hazmat Shipper
1. TSA Universal Communications Interface (UCI)
2. Web interface with hazmat shippers/carriers
FedTrak™
Tier 1 HSSM Truck Security
E-Manifest + Route Plan + Truck Location + Alerts
What is the truck carrying?
What is the shipment risk profile?
Who is driving the truck?
What is the truck's location?
Is there a problem? What?
What is the truck's destination?
What route has the truck followed?
Is the truck off-route?
3. Data integration: location, alerts, e-manifests, e-routes
4. Business rules engine: dynamic risk profiling
5. Business workflow, data presentation and operations center systems
North American Transportation Security Center
Transportation Security Administration
State Action Agency (Fusion Center)
Hazmat (Tier 1 HSSM) Carriers
First Responders
6. Interface with TSA, state action agencies, hazmat carriers, and first responders

1.2 Shippers, carriers, and fleet tracking vendors have to deploy "smart truck" technology and submit data to enable a truck tracking center.

To succeed, a hazmat truck tracking center needs data. Hazmat carriers have to deploy smart truck technology, and shippers, carriers, and truck tracking vendors must submit

A hazmat truck tracking center is dependent on data flow from shippers, carriers and fleet tracking vendors. Data is the raw product that a truck tracking center converts into actionable intelligence. Efficient and timely processing of data gives the center the ability to answer the questions presented in Figure 2.1 and allows it to effectively support government action agencies when a transportation security incident is declared.

However, a truck tracking center will fail unless smart truck technology is widely deployed and shippers, carriers and fleet tracking vendors submit data to the truck tracking center. Currently, there is no regulatory requirement that hazmat shippers deploy smart truck technology or submit data to a truck tracking center. [1]

Industry groups have advocated voluntary measures for hazmat technology deployment and data reporting. However, voluntary industry measures – while conceptually appealing – rarely work. The FMCSA FOT study acknowledged the problem of industry-led voluntary programs by suggesting that "government intervention" (e.g. regulations) will be needed to stimulate smart truck technology deployment and data reporting. This argument for "government intervention" is buttressed by DHS's recent experience in its

[1] The exceptions are munitions and radioactive material shipments. However, these shipments represent only a small fraction of the total number of high-risk hazmat shipments in the U.S.

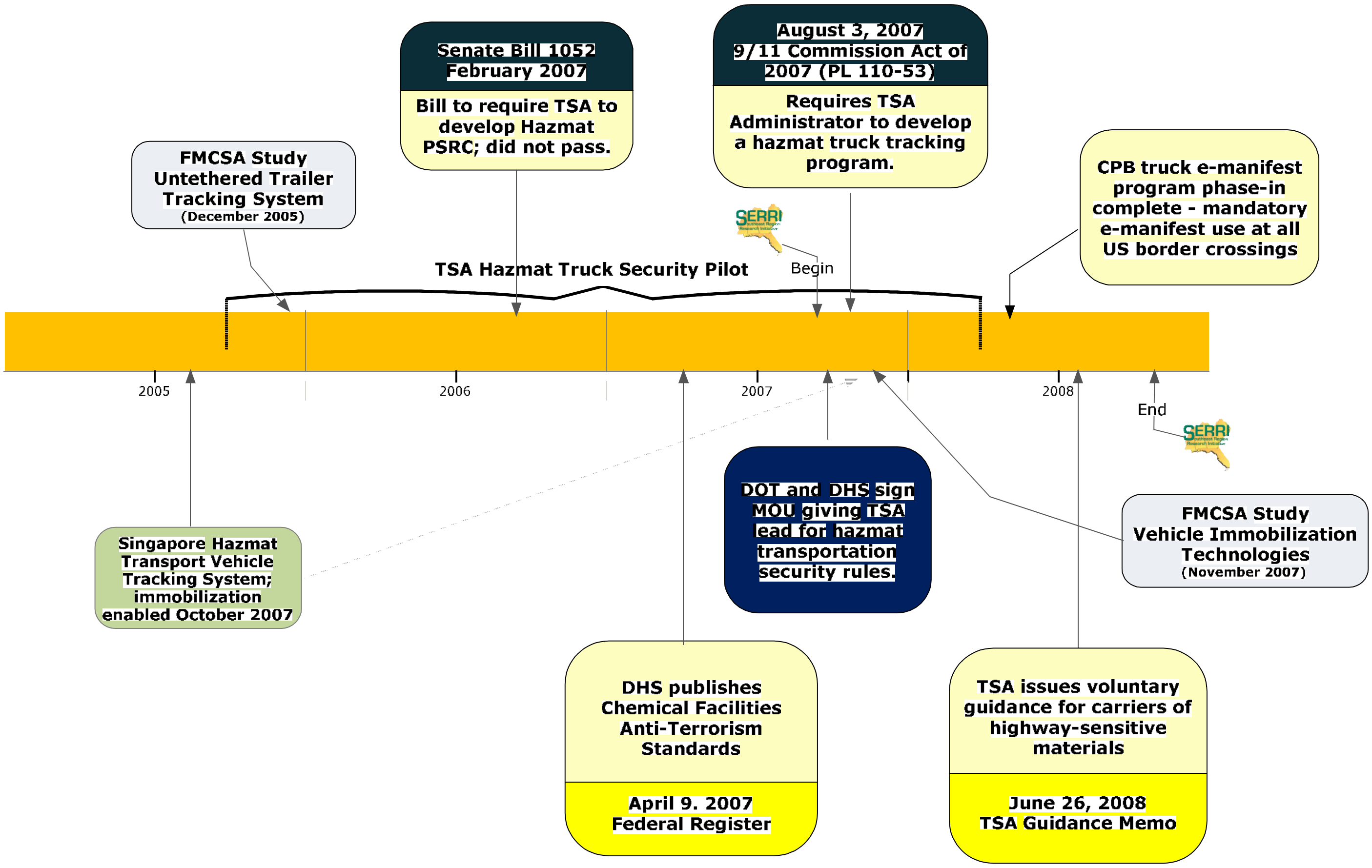
efforts to beef up security at chemical production plants in urban areas. In that case, an industry-led voluntary initiative to upgrade chemical plant security resulted in such a tepid industry response that DHS had to take the program back and issue regulations to require chemical companies to institute security programs.

It is unlikely that hazmat trading partners will voluntarily submit data to a truck tracking center.

1.3 The HTSP technology prototype design reflected assumptions about technology deployment and data reporting.

Figure 1.2 shows the timeline of events surrounding the HTSP project. The HTSP project began in October 2005 and ended April 2008.

Figure 1.2 The HTSP project began October 2005 and ended April 2008.



FMCSA Study Untethered Trailer Tracking System (December 2005)
Senate Bill 1052 February 2007
Bill to require TSA to develop Hazmat PSRC; did not pass.
August 3, 2007 9/11 Commission Act of 2007 (PL 110-53)
Requires TSA Administrator to develop a hazmat truck tracking program.
CPB truck e-manifest program phase-in complete - mandatory e-manifest use at all US border crossings
SERRI
Begin
TSA Hazmat Truck Security Pilot
2005
2006
2007
2008
End
SERRI
Singapore Hazmat Transport Vehicle Tracking System; immobilization enabled October 2007
DOT and DHS sign MOU giving TSA lead for hazmat transportation security rules.
FMCSA Study Vehicle Immobilization Technologies (November 2007)
DHS publishes Chemical Facilities Anti-Terrorism Standards
April 9. 2007 Federal Register
TSA issues voluntary guidance for carriers of highway-sensitive materials
June 26, 2008 TSA Guidance Memo

The FMCSA's Field Operations Test was completed a year before the HTPS project began. While the FOT project report suggested that regulations should drive technology deployment and data reporting – especially in light of positive ROI generated by smart truck technology – the time was not right in late 2005 for a regulatory push by federal agencies. The responsibility for regulation of hazmat shipments was in transition from DOT to DHS, and a number of thorny technical and regulatory uncertainties existed. The results of the FMCSA field tests on vehicle immobilization systems and untethered trailer tracking systems were not yet available, and the concept of operations for a hazmat truck tracking center had been only mildly developed in the FOT. Moreover, there was a great deal of uncertainty about the role that regulations would play in securing the nation's hazmat supply chain.

In late 2005 when the HTSP began, there was uncertainty about technology and regulatory issues.

The HTSP project was hugely successful in that it proved that a hazmat truck tracking center is feasible from a technology perspective.

Even though the HTSP prototype's functionality was limited by industry participation, the HTSP pilot was highly successful. It proved that a hazmat truck tracking center is technically feasible and that smart truck technology can be crafted into an effective and efficient system for tracking hazmat shipments. However, the pilot fell far short of advancing a regulatory and implementation framework that would allow TSA to move forward with its hazmat truck tracking program. This is not a criticism of the HTSP pilot or the work done on it – development of a framework for implementing TSA's hazmat truck tracking program was not part of the mission of the project team.

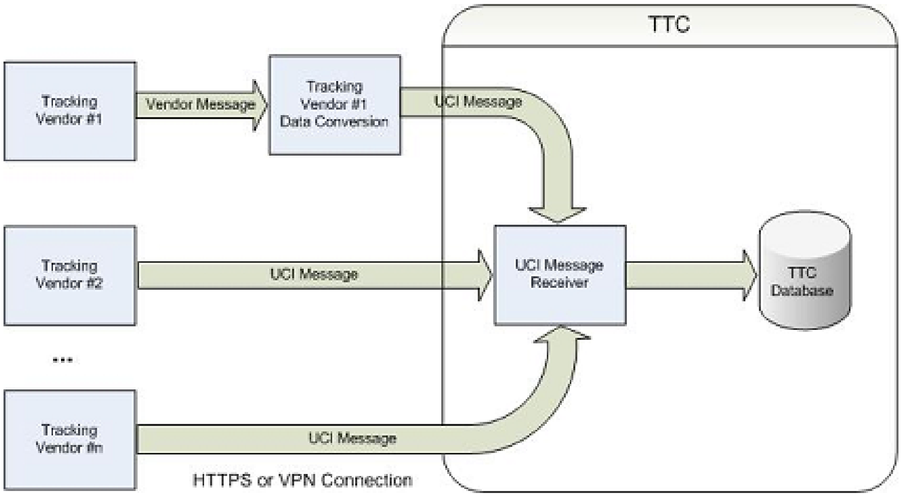
1.4 The HTSP technology prototype used an XML communications interface based on the IEEE 1512 standards. [2].

The HTSP contractor was given the following direction by TSA for constructing a messaging interface for the HTSP.

> *"Develop and demonstrate a set of communication protocols that shall allow alerts and tracking information to be transmitted from commercial in-use truck tracking systems to a prototype truck tracking center in order to enhance the ability of state, local, and federal authorities to identify and respond to Transportation Security Incidents (TSIs). The interface shall also be capable of receiving and processing information from all other commercially available truck tracking systems."* [3]

Appendix A contains links to TSA Universal Communications Interface design documents. **Figure 1.3** illustrates the high-level design for the communications interface that was built for the HTSP. Under this design scenario, fleet tracking vendors are required to report data in a form and format consistent with the communications standard set by the truck tracking center.

Figure 1.3 Fleet tracking vendors build to a standard communications interface.



The HTSP communications interface was built using the IEEE-1512 Standard for Common Incident Management Message Sets for Use by Emergency Management Centers (known as the 1512 Base Standard) and the IEEE-1512 Standard for Hazardous

[2] Section 4.5.4 is taken from, "*Hazmat Truck Security Pilot – Final Report – Objective 3, Communication Interface Development and Testing";* April 11, 2008; General Dynamics Advanced Information Systems.

[3] A transportation security incident (TSI) is defined by TSA as a security incident resulting in significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area (46 USC 701).

Material Incident Management Message Sets for use by Emergency Management Centers (known as the 1512.3 Standard). It was also built to conform to the National Transportation Communications for ITS Protocol (NTCIP).

The HTSP communications interface was built using IEEE 1512.3 standards for hazmat incidents.

The 1512 Base standard provides messages and data that are common to one or more members of the 1512 family of standards, which also includes Traffic Incident Management (1512.1) and Public Safety Incident Management (1512.2). IEEE-1512.3 provides unique messages and data for the communication of hazardous material related incident information.

An interface requirements specification (IRS) and an Interface Control Document (ICD) were prepared to support the development of the HTSP interface standard.

The design of the UCI is based on a concept of events and alerts with the interface receiving and displaying tracking information and specialized alerts. With this in mind, the HTSP contractor defined an event to be a specific shipment, from gate-out to gate-in. A gate-out message indicates the start of the shipment event and a gate-in message indicates the end of the shipment event. Position updates for this shipment are then treated as updates to the shipment event. Other message types, such as panic button presses, are treated as alerts associated with the specific shipment event.

The UCI processes events and alerts associated with events. An event is a specific shipment – from gate out to gate in.

The UCI consists of three IEEE-1512 messages and associated sub-messages.

- **Message Type 1 - Incident Description (IDX) message**. The IDX message allows event data (messages) to be sent to the central truck tracking center application. The design of the UCI treats any shipment as an incident or event, with the start of the incident being triggered by a gate out indication. The IDX message will always contain the following information:
    - Incident or Event ID – This is a globally unique identifier that was assigned to each incident at gate out.
    - Timestamp – This is the time the message was sent to the TTC.
    - Event Type – Event type is a standardized list of phrases describing the type of event. The event type may change during the course of an incident. For example a shipment being tracked would have an event type of 'position report' initially. If the driver then hit the panic button, the event type would change to 'driver alarm', while the Incident ID remained the same. **Figure 1.4** lists the event types that were supported by the HTSP

An incident description message is used to signal different event types including gate out, position report, driver alarm, etc.

Figure 1.4 The HTTP communications interface recognizes 18 event types.

shipment off course	position report	driver alarm
vehicle hijack	unexpected cargo weight change	unexpected cargo temperature change
attempted security bypass	automatic vehicle throttle down	automatic vehicle stopping
unexpected trailer separation	unauthorized system disabling	overdue shipment
entered geo-fence	exited geo-fence	accident involving a semi trailer
cargo data	location – the reported latitude and longitude position at the time of the message	emergency contact number – the number to call for the carrier if an emergency situation occurs.

The standard requires that each IDX message contain at least one of four IDX sub-messages.

IDX Sub-Message 1 – Cargo Document

The incident description message is used to describe a vehicle's cargo (type, quantity) .

The Cargo Documents message is used to convey the information typically found in commercial shipping papers. The Cargo Documents message contains the following information:

- Cargo Vehicle ID – An ID number that associates the cargo documents to a cargo vehicle.
- Cargo Unit ID – An ID number that associates the cargo documents to a cargo unit.
- Material ID Number – The UN number assigned to the material being shipped. This is also the placard number(s) that must be displayed on the truck.
- Quantity – The quantity of the material being shipped. Some of the more common accepted values are grams, kilograms, ounces, pounds, tons, fluid ounces, gallons, milliliters and liters.

IDX Sub-Message 2 – Cargo Vehicle

The incident description message is used to describe a vehicle's identification and provide information on the driver.

The Cargo Vehicle message is used to describe the vehicle associated with the incident. The Cargo Vehicle message can be used to identify any type of vehicle that could haul cargo. The Cargo Vehicle message contains the following information:

- Cargo Vehicle ID – An ID number assigned to the vehicle.
- Cargo Unit ID's – ID numbers assigned to cargo units associated with the vehicle.
- Vehicle Information – Provides the basic information to help in identifying a vehicle. The UCI is using make, color, license plate and registration number.
- Driver Information – Provides information to identify a vehicles driver. Currently, the interface supports the following information; the name and address of the driver and the name and address of the company the driver works for. The HTSP contracted suggested to the IEEE1512 committee that it consider changing the driver information to use the GJXDM person model. If adopted this change would include social security number, date of birth and detailed driver's license information.

IDX Sub-Message 3 – Cargo Units

The Cargo Units message is used to describe the trailer or unit associated with a cargo vehicle. The Cargo Units message contains the following information:

The incident description message is used to describe a vehicle's cargo units including trailers.

- Cargo Vehicle ID – The ID of the vehicle associated with the cargo unit, if one exists.
- Cargo Unit ID – the cargo units assigned ID.
- Contents – If a trailer is un-tethered, the contents of the trailer can be described here.

IDX Sub-Message 4 – Resource Assignment

The Resource Assignment message is used to provide origin and destination information for the vehicle. The message contains the following information:

The close message indicates gate in status for the shipment – i.e. that the trip has ended.

- Origin, Destination – Provided the ability to describe the origin and/or destination. Currently, we are only asking for city, state due to carrier reluctance to provide more information. The interface can support a full mailing address.
- In addition this message is capable of receiving detailed GPS information, such as speed and heading, if it were available and of interest to TSA.

- **Message Type 2 – Close Message.** The Close Message is used to indicate that a given event has been closed from the perspective of the center sending the message. This message will be sent when a gate in event occurs or when a truck tracking center operator manually closes an incident.
- **Message Type 3 - Watch For Message.** The Watch For message was added to the UCI to support risk-based profiling of hazmat shipments. UCI data is provided to

a risk analysis system. In the case of the HTSP, a commercial product, Fdfolio™, served as a business rules/risk engine for the HTSP. The risk analysis system analyzes the data and assigns a risk score based on different factors, such as the material being shipped or the vehicles location. The risk analysis system then sends the Watch For message to the UCI. The message contains the following information:

- A hyperlink to the risk system's web page associated with the reported score. This provides an operator the ability to directly view and update the reasons for a risk assessment.
- A risk level score that provides a numerical value for assessing a shipments risk that corresponds to the DHS threat levels.
- A quick summary of the reasons for the risk score.
- The recommended instructions associated with a particular risk score.

The watch for message is generated by the HTSP's risk engine to alert the operator that a significant event raising the risk profile of the shipment has occurred.

1.5 The HTSP's Transportation Event Analysis and Management System processes and displays event-based data. [4]

The HTSP's Transportation Event Analysis and Management System (TEAMS) is an event-based system that stores and displays event-based information received in messages from transportation-related systems and sends notifications when messages identifying new events are received. TEAMS automatically collects data in real-time from commercial fleet tracking vendors. Fleet tracking vendors that participated in the HTSP included Qualcomm, PeopleNet, and Safefreight.

The HTSP's Transportation Event Analysis and Management System (TEAMS) is an event-based system that stores and displays event-based information received in messages from transportation-related systems. vendors.

The HTSP contractor developed a basic version of TEAMS prior to its work for TSA on the Hazmat Truck Security Pilot project. TEAMS – as it stood prior to modification for the TSA project – had the following functionality.

- TEAMS is an event-based system that stores and displays event-based information received in messages from transportation-related systems and sends notifications when messages identifying new events are received. TEAMS displays event information in textual, pictorial, and geospatial formats.
- TEAMS uses a web service to receive event-based XML messages. When a message is received that contains information about an event not in the TEAMS database, a new event is created in the database. When a message is received that contains information about an event already existing in the TEAMS database, the information for that event is updated in the TEAMS database.
- TEAMS provides human-readable output in HTML so that a user only requires a web browser to view the current state of events. Thus, authorized users can access TEAMS anywhere a computer and internet connectivity is available with appropriate security (VPN). TEAMS controls access by authenticating users based on user IDs and passwords. Event information is presented in textual and pictorial format. Event location is presented in geospatial format.
- TEAMS uses ESRI-formatted map data on which event location is overlaid. The map display can be controlled using zoom and scroll controls.
- TEAMS uses email to notify users of new events. Email messages can be sent to desktop computers, handheld computers, and SMS- enabled cellular telephones.
- TEAMS is a Java-based application that utilizes a web server, a J2EE application server (currently SUN), and a relational database (currently Microsoft SQL Server) to process, store, and present event information. TEAMS can be easily modified to process, store, and present any event-based information.

TEAMS automatically collects data in real-time from commercial truck tracking vendors.

The HTPS contractor made the following enhancements to TEAMS to meet TSA's HTSP objectives.

- User interface enhancements. The TEAMS user interface was enhanced to support unique needs of the HAZMAT truck tracking application. New data views and functionality were added.

[4] Sections 2.5 – 2.11 are taken from, "*Hazmat Truck Security Pilot – Final Report – Objective 2, Truck Tracking Center Prototype";* April 11, 2008; General Dynamics Advanced Information Systems.

Additional functionality was added to the basic TEAMS product to adapt it to use as a hazmat truck tracking tool.

- Modifications to support risk assessment. TEAMS was enhanced to support working in an integrated environment with a risk assessment tool (FDfolio). These included database enhancements, communications enhancements, display enhancements, and the ability for users to access the risk assessment tool.
- Vehicle tracking. TEAMS was enhanced to support vehicle tracking including the ability to display vehicle history locations graphically.
- Alerting. TEAMS was enhanced to support the presentation of alerts needed to notify operators when new events or information are available.
- Access control. TEAMS was enhanced to provide a mechanism for setting passwords and restricting access to authorized users.
- Material handling guidance. TEAMS was upgraded to allow TTCP operators to access information regarding HAZMAT materials and appropriate emergency responses.
- HAZMAT data storage and display. TEAMS was upgraded to support the acquisition, storage, and display of HAZMAT truck identification and HAZMAT cargo information.
- Access to map overlays. TEAMS was enhanced to allow access to orthographic maps with imagery of locations of interest.
- Geo-fencing. TEAMS was upgraded to support defining geo-fences by demarcating areas within any polygonal shape and determination of when HAZMAT trucks violate defined geo-fences. The capability handles both exclusionary and inclusionary geo-fences.
- Local Public Safety Answering Point (PSAP) identification. TEAMS was upgraded to present PSAP contact information for an event based on the location of the HAZMAT truck in relation to local PSAP jurisdictions.
- Points of interest. TEAMS was upgraded to provide determination of and access to points of interest (e.g., schools, hospitals, power plants) near an incident.
- Current weather. TEAMS was enhanced to provide access to current weather information in the vicinity of HAZMAT security events.

1.6 The communications architecture for the HTSP technology prototype supports efficient dataflow between system components.

A key system feature that TSA required in the HTSP was the ability of the prototype to share critical information across disparate systems in real time. **Figure 1.5** illustrates the communications architecture that was deployed in the pilot program. The system uses the UCI for data communications between the truck tracking centers, TEAMS and FDfolio™. The interfaces are event-based. When a new event, either an alert or position update is generated by a connected truck tracking system, FDfolio™ provides an updated assessment of risk and TEAMS determines whether a geo-fence violation has occurred and updates displays. Truck tracking center operators and TSA Watch Officers (i.e., TSA person responsible for managing alerts) are able to use TEAMS to "drill down" to view FDfolio™ displays allowing review and management of rules that may have created a risk-based alert. Center operators and Watch Officers are also able to provide PSAPs with secure access to TEAMS displays in support of emergency response actions.

1.7 The HTSP technology prototype was built around a "concept of operations" workflow.

A functional block diagram of TEAMS is presented in **Figure 1.6**. It shows the data type and flow through the system from the data source to system users. This is a high level look at the system from an information management perspective.

A Concept of Operations (ConOps) describes the characteristics of a system from the users' point of view. For the HTSP, the Concept of Operations specifies the operational requirements for implementing a centralized truck tracking center and coordination and

Figure 1.5 HTSP Prototype Communications Architecture

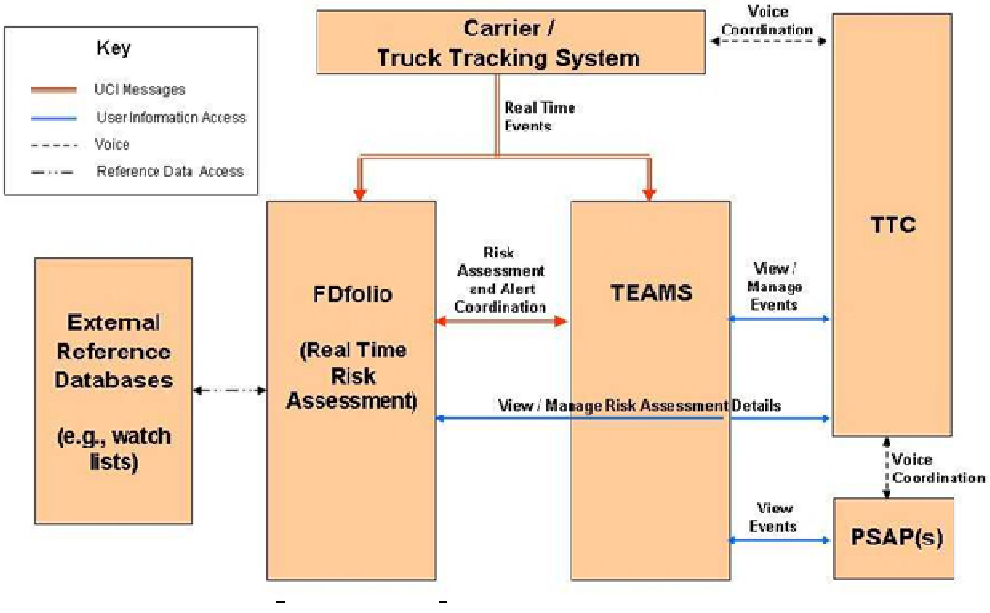

Key
UCI Messages
User Information Access
Voice
Reference Data Access
Carrier / Truck Tracking System
Voice Coordination
Real Time Events
TTC
External Reference Databases (e.g., watch lists)
FDfolio (Real Time Risk Assessment)
Risk Assessment and Alert Coordination
TEAMS
View / Manage Events
View / Manage Risk Assessment Details
Voice Coordination
View Events
PSAP(s)

Figure 1.6 TEAMS exchanges data with other components of the prototype.

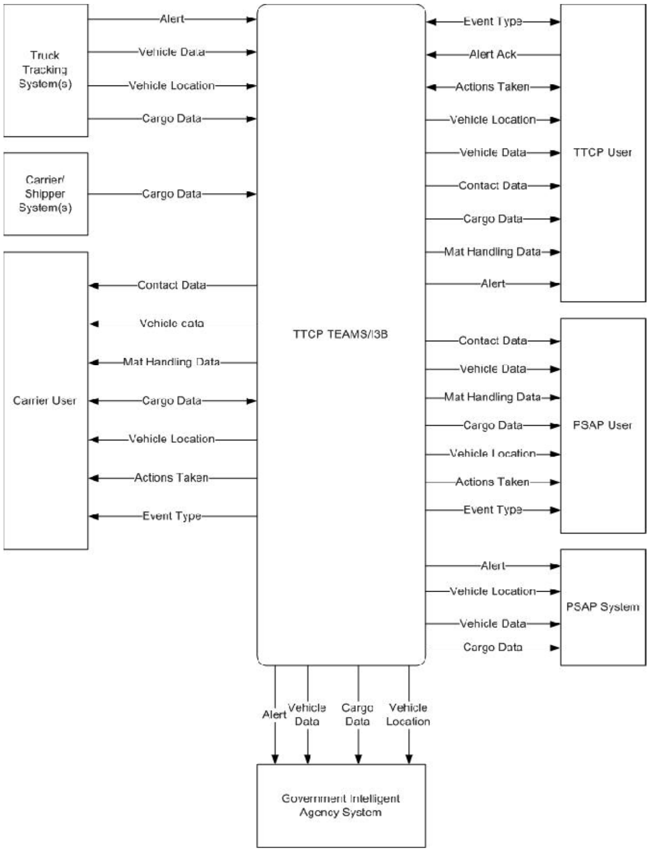
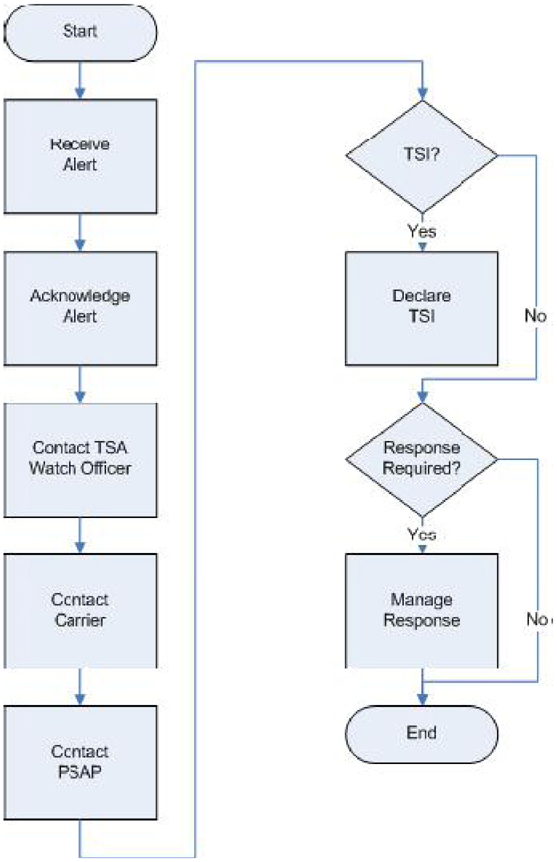


Figure 1.7 TEAMS supports the HTSP's "concept of operations" workflow.



management of Transportation Security Incidents (TSIs). As illustrated in **Figure 1.7,** the basic ConOps adopted for the HTSP was as follows:

The HTSP ConOps plan relies heavily on telephonic communications. PSAPs – not state agencies – manage local response decision-making under the plan.

1. A Universal Communications Interface message is received by the truck tracking center. The truck tracking center processes the message to determine if it is a routine position report message or an alert message. The message is also forwarded to the risk assessment engine, whether it is a routine message or an alert, to be assessed based on its data content

2. If the message is an alert, or if the risk score causes an alert, the truck tracking center operator contacts the TSA watch officer by phone to make sure TSA is aware of the situation.

3. The truck tracking center operator creates a three way conference call by calling the carrier, using a number provided by the carrier.

4. If the carrier is aware of the situation and it is deemed not to be a TSI, then the process of resolving the event is left to the carrier's normal response plans.

5. If the carrier cannot be contacted, or if the carrier is contacted but isn't sure if the event is a security situation, then the tracking center determines the Public Safety Answering Point (PSAP) with jurisdiction for the event and includes them in the conference call.

6. TSA, the carrier and the PSAP collectively discuss the event to determine if it is a security situation or not. If a TSI is declared then TSA takes over the responsibility for handling the event.

The notifications of hazmat transportation events are termed "alerts". TEAMS receives data from fleet tracking vendors and carrier/shipper systems through the UCI. TEAMS uses this data to recognize and initiate an alert when a new incident is identified. An alert mechanism is included in the TEAMS application and is employed to notify the truck tracking center operators, and other designated workstations (i.e., the DHS TSOC) of the new incident. The truck tracking center operator uses TEAMS to view all related data, manage the required notifications, log all actions associated with the event, and monitor the TSI status until closed.

The TEAMS application is the primary user interface to truck tracking center data. The UCI collects data from various truck tracking and carrier manifest sources to support truck tracking center operations. Certain data elements collected from the field are used to indicate/notify the onset of transportation events which may evolve into a transportation security incident (TSI) – such as panic button activation, cargo monitoring exception, off route or geo-fence violation. Notifications may also be telephonically called into the truck tracking center by TSA, a carrier, or other federal/state/local government agency.

There is a working definition for "transportation security incident" but the criteria that TSA and others would use to decide if an incident should be declared as a TSI was not described in the HTSP project report.

TEAMS is used to implement workflows and specific processes. In TEAMS, alert and notification information is presented to the truck tracking center operator on a workstation screen. On screen is a list of persons to be notified (i.e., TSA Watch Officer, carrier contact, Public Safety Answering Point (PSAP), etc.). Each listing provides a method(s) of notification, such as telephone call, e-mail, fax, etc. (or any combination of these). The TTC System allows for electronic notification via e-mail, cell phone SMS, and fax. In TEAMS, a "Contacted/Sent" toggle button is associated with each listed person/agency to be notified. When the "Contacted" button is clicked, a check mark appears in the box, indicating that a call has been placed to the contact and a record will be made of this call in the Action Log. The Action Log contains a complete list of all entries made into the system by external systems or users. Similarly, when the "Sent" button is clicked the listed electronic notification (e.g., fax or e-mail) message will automatically be sent and a record made of the transaction in the Action Log. The user is also provided with alternates for additional (adjoining) PSAP notification to ensure that entities are notified if the primary contacts are not available.

Initial transportation event notifications are evaluated through the process described in the following paragraph to determine if a TSI should be declared, and what should be an appropriate response. The TTC may help coordinate a public safety response even though a TSI is not declared.

When a new event is received, the truck tracking center operator reviews the data and begins the notification process. In TEAMS, on the TSI Details screen, the "First Contacts" section provides all necessary information to contact and notify TSA staff, carriers, first responders, and any other entity designated in the procedures established. In the same "First Contacts" listing, other contact information, such as office and cell phone numbers, is displayed. The dispatcher makes a telephone call to each "Required" and "Requested" contact, and logs each successful notification in the TEAMS application.

1.8 TEAMS is a Java-based server application composed of two major components: the user interface and data services.

TEAMS is a Java-based server application, running on the JBoss 2EE server, composed of two major components: the user interface and the data services. For developing the TEAMS user interface, JavaServer Faces with some JavaScript code was used for client-side interaction. JavaServer Faces is a technology that simplifies building user interfaces for Java server applications by providing reusable components, simplified page navigation, and a drag and drop graphical user interface designer.

Another benefit of JavaServer Faces is that at runtime, all JavaServer Faces components get decompiled into standard HTML tags on the user's browser. This approach increases the accessibility of TEAMS versus an approach that would have used an embedded component such as a Java Applet or a Flash Application.

The data services software module was written as a J2EE application with an Oracle database providing the data storage. Rather than coding specifically for Oracle and using Oracle SQL queries for data storage and retrieval, the object/relational persistence engine known as Hibernate 5 was used. Hibernate provides the ability to change the database without having to change any of the TEAMS query code. A simple modification to a configuration file allows TEAMS to use another database such as Microsoft SQL Server or MySQL if needed.

The data services software module is used by TEAMS to store data when a message is received and to retrieve data when it is requested. Data is received by the data services module through the UCI interface. When the data is received, the 1512 XML data message is validated for conformance to the 1512 schema and then the data is parsed from each XML field.

One important security decision that was made was to do message validation at the application level rather than the Web Service Definition Language (WSDL) level. Had validation been done at the WSDL level, it would have exposed the schema in the WSDL file. Assuming that an intruder would be able to correctly guess a username and password that would allow access to the WSDL, that intruder would be able to inject false data into the system because the schema would be available in the WSDL. By doing the data validation at the application level, access to the schema could be restricted to only those that received the UCI documentation, adding an extra layer of security that prevents the injection of incorrect data.

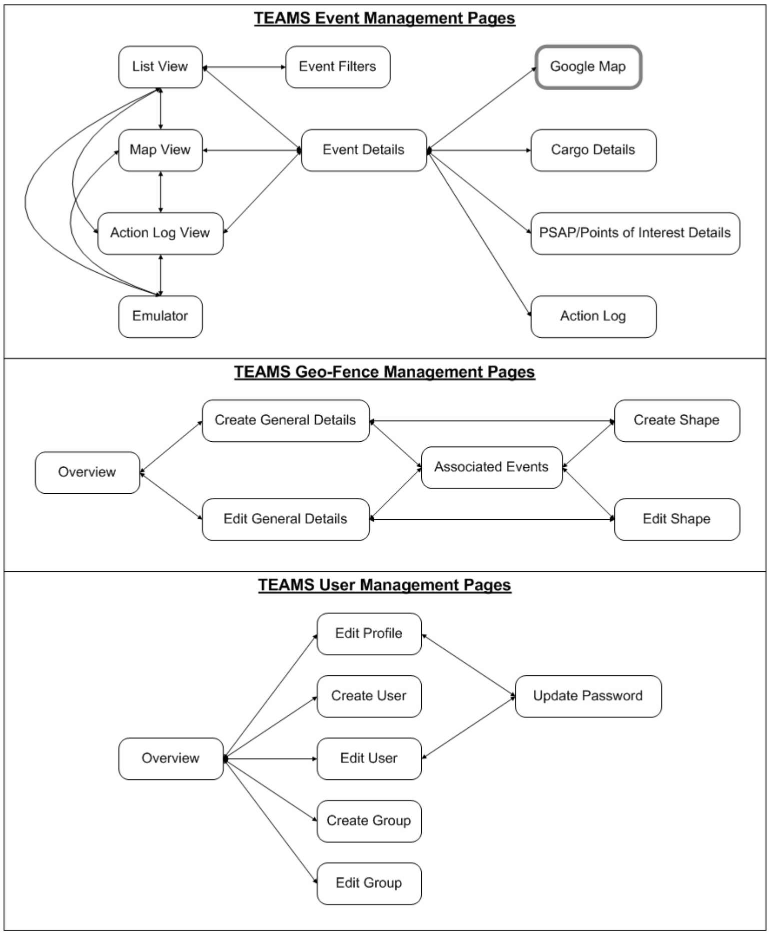
After the data has been parsed from the XML message, some geospatial analysis occurs before all of the data is saved to the database. This geospatial analysis includes reverse geo-coding, PSAP boundary lookup, and geo-fence violation detection. Once the geospatial analysis takes place, the data is saved to the database. The data services software also provides a web service interface that is used to populate the TEAMS graphical user interface with data.

1.9 The TEAMS user interface is composed of multiple web pages that can be navigated to view event data, user account data, and geo-fence data.

The TEAMS user interface is composed of multiple web pages that are connected to each other and can be navigated through to view event data, user account data, and geo-fence data. **Figure 1.8** provides a high level overview of the interaction between the various pages that form the TEAMS applications.

The TEAMS user interface is composed of multiple web pages that are connected to each other and can be navigated through to view event data, user account data, and geo-fence data.

Figure 1.8 The TEAMS user interface connects multiple webpages.



1.9.1 List view displays high level information for all active shipments.

Once authenticated to TEAMS, the user will arrive at the List View page. As illustrated in **Figure 1.9**, this page contains a list of all active events currently being tracked by the TEAMS software. For each event in the list there is a designation of whether or not the event has been declared a transportation security incident (TSI). Additionally, the event's risk level, the event ID, the date and time the most recent update was received, the type of event, the status of the event, address, city, state, and estimated population impact are shown in the list.

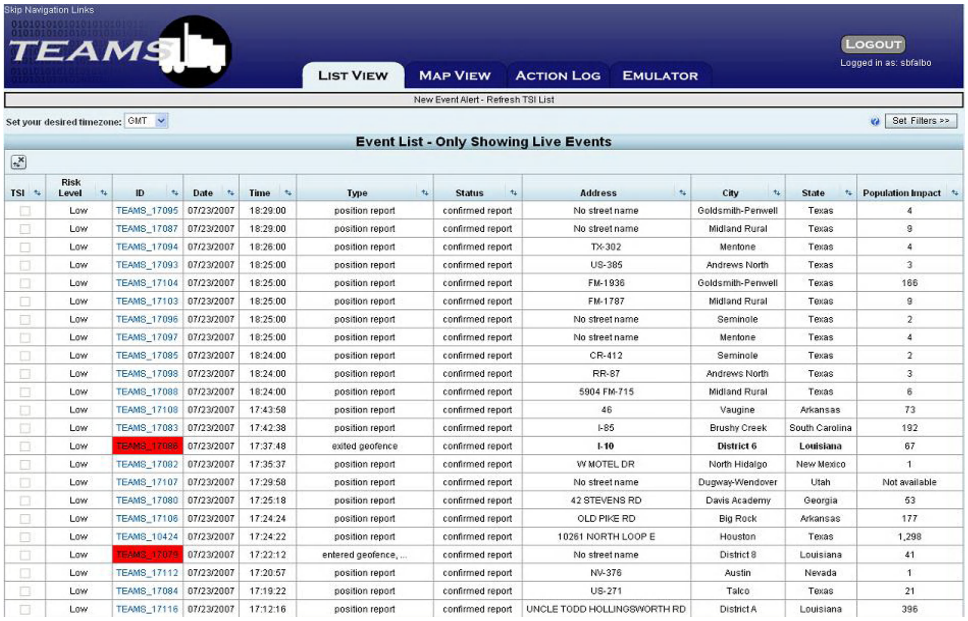
The event ID displayed in the list is a hyperlink and by clicking on this link a user will navigate to the Event Details page for that event. Also displayed on the List View page are tabs that a user can click on to navigate to the Map View page, Action Log page, or Emulator page. A user can filter the list of events being shown by clicking on the 'Set Filters' button to navigate to the Event Filters page. A user can change the time zone in which times are displayed throughout TEAMS by selecting a time zone from the drop down on the List View. If event data is received by the UCI that triggers an alert, the "New Event Alert – Refresh TSI List" button will begin flashing indicating that the user needs to update the event list. This new alert button is displayed on all pages in the main TEAMS application.

The map view shows all active shipments being tracked on a map.

1.9.2 The map view page displays the map location of active shipments.

The Map View page illustrated in **Figure 1.10** is similar in functionality to the List View page in that gives a high level overview of all of the active shipments currently being tracked by TEAMS. It differs from the List View in that all of the shipments are

Figure 1.9 Teams list view page



Set your desired timezone: GMT

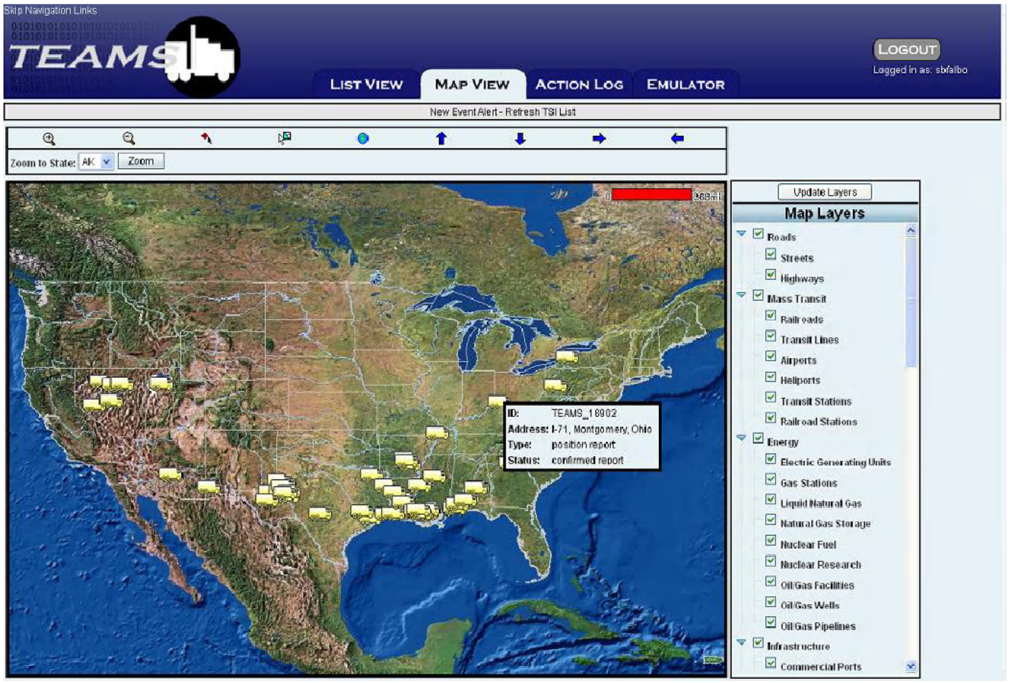
Event List - Only Showing Live Events

TSI	Risk Level	ID	Date	Time	Type	Status	Address	City	State	Population Impact
☐	Low	TEAMS_17095	07/23/2007	18:29:00	position report	confirmed report	No street name	Goldsmith-Penwell	Texas	4
☐	Low	TEAMS_17087	07/23/2007	18:29:00	position report	confirmed report	No street name	Midland Rural	Texas	9
☐	Low	TEAMS_17094	07/23/2007	18:26:00	position report	confirmed report	TX-302	Mentone	Texas	4
☐	Low	TEAMS_17093	07/23/2007	18:25:00	position report	confirmed report	US-385	Andrews North	Texas	3
☐	Low	TEAMS_17104	07/23/2007	18:25:00	position report	confirmed report	FM-1936	Goldsmith-Penwell	Texas	166
☐	Low	TEAMS_17103	07/23/2007	18:25:00	position report	confirmed report	FM-1787	Midland Rural	Texas	9
☐	Low	TEAMS_17096	07/23/2007	18:25:00	position report	confirmed report	No street name	Seminole	Texas	2
☐	Low	TEAMS_17097	07/23/2007	18:25:00	position report	confirmed report	No street name	Mentone	Texas	4
☐	Low	TEAMS_17085	07/23/2007	18:24:00	position report	confirmed report	CR-412	Seminole	Texas	2
☐	Low	TEAMS_17098	07/23/2007	18:24:00	position report	confirmed report	RR-87	Andrews North	Texas	3
☐	Low	TEAMS_17088	07/23/2007	18:24:00	position report	confirmed report	5904 FM-715	Midland Rural	Texas	6
☐	Low	TEAMS_17108	07/23/2007	17:43:58	position report	confirmed report	46	Vaugine	Arkansas	73
☐	Low	TEAMS_17083	07/23/2007	17:42:38	position report	confirmed report	I-85	Brushy Creek	South Carolina	192
☐	Low	TEAMS_17086	07/23/2007	17:37:48	exited geofence	confirmed report	**I-10**	**District 6**	**Louisiana**	67
☐	Low	TEAMS_17082	07/23/2007	17:35:37	position report	confirmed report	W MOTEL DR	North Hidalgo	New Mexico	1
☐	Low	TEAMS_17107	07/23/2007	17:29:58	position report	confirmed report	No street name	Dugway-Wendover	Utah	Not available
☐	Low	TEAMS_17080	07/23/2007	17:25:18	position report	confirmed report	42 STEVENS RD	Davis Academy	Georgia	53
☐	Low	TEAMS_17106	07/23/2007	17:24:24	position report	confirmed report	OLD PIKE RD	Big Rock	Arkansas	177
☐	Low	TEAMS_10424	07/23/2007	17:24:22	position report	confirmed report	10261 NORTH LOOP E	Houston	Texas	1,298
☐	Low	TEAMS_17079	07/23/2007	17:22:12	entered geofence, ...	confirmed report	No street name	District 8	Louisiana	41
☐	Low	TEAMS_17112	07/23/2007	17:20:57	position report	confirmed report	NV-376	Austin	Nevada	1
☐	Low	TEAMS_17084	07/23/2007	17:19:22	position report	confirmed report	US-271	Talco	Texas	21
☐	Low	TEAMS_17116	07/23/2007	17:12:16	position report	confirmed report	UNCLE TODD HOLLINGSWORTH RD	District A	Louisiana	396

The list view provides tabulated information on all active shipments that the system is tracking.

displayed on a map of the United States instead of in a list format. To obtain overview information about an event a user can hover over the event's icon on the map to be shown a popup containing the event ID, address, type, and status. The Map View page provides navigational map tools as well as a tool that allows a user to click on an event's icon to navigate to the Event Details page to get further event information. The Map View also contains controls that allow a TEAMS user to turn particular map overlays on and off as desired. Also displayed on the Map View page are tabs that a user can click on to navigate to the List View page, Action Log page, or Emulator page.

Figure 1.10 TEAMS map view page.



Zoom to State: AK

ID: TEAMS_16902
Address: I-71, Montgomery, Ohio
Type: position report
Status: confirmed report

Map Layers

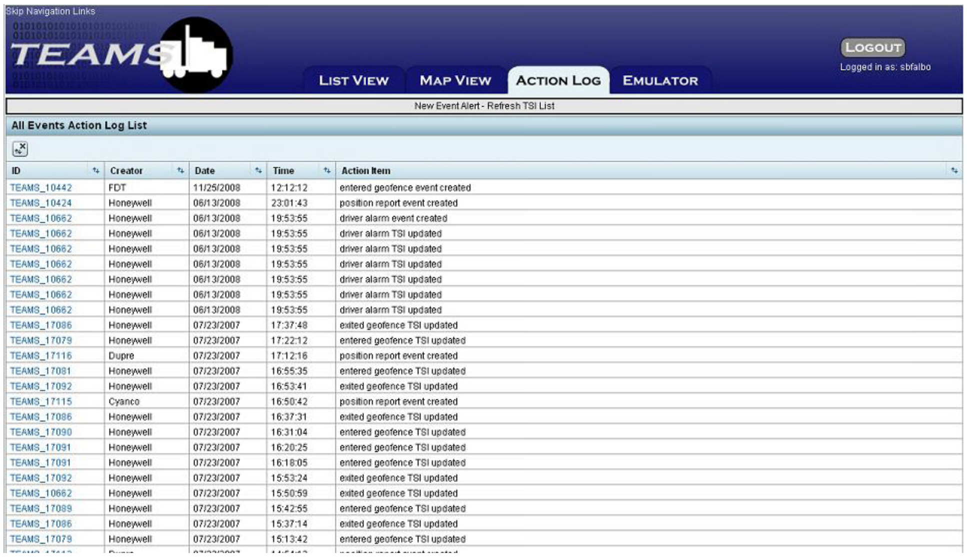
- ☑ Roads
  - ☑ Streets
  - ☑ Highways
- ☑ Mass Transit
  - ☑ Railroads
  - ☑ Transit Lines
  - ☑ Airports
  - ☑ Heliports
  - ☑ Transit Stations
  - ☑ Railroad Stations
- ☑ Energy
  - ☑ Electric Generating Units
  - ☑ Gas Stations
  - ☑ Liquid Natural Gas
  - ☑ Natural Gas Storage
  - ☑ Nuclear Fuel
  - ☑ Nuclear Research
  - ☑ Oil/Gas Facilities
  - ☑ Oil/Gas Wells
  - ☑ Oil/Gas Pipelines
- ☑ Infrastructure
  - ☑ Commercial Ports

The action log page provides information on the things that "have been done" in tracking active shipments.

1.9.3 The action log view page displays log entry data for active shipments.

The Action Log View page illustrated in **Figure 1.11** shows all of the action log entries for each active shipment currently in TEAMS. Each time the TEAMS database is updated, an entry is automatically made in the Action Log. A TEAMS user can also manually make an entry in the action log to record anything not entered automatically

Figure 1.11 TEAMS action log view page.



All Events Action Log List

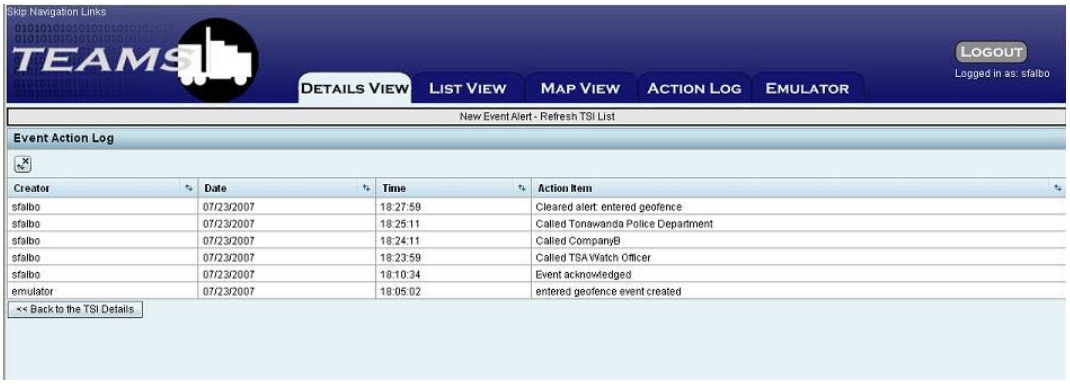
ID	Creator	Date	Time	Action Item
TEAMS_10442	FDT	11/25/2008	12:12:12	entered geofence event created
TEAMS_10424	Honeywell	06/13/2008	23:01:43	position report event created
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm event created
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_10662	Honeywell	06/13/2008	19:53:55	driver alarm TSI updated
TEAMS_17086	Honeywell	07/23/2007	17:37:48	exited geofence TSI updated
TEAMS_17079	Honeywell	07/23/2007	17:22:12	entered geofence TSI updated
TEAMS_17116	Dupre	07/23/2007	17:12:16	position report event created
TEAMS_17081	Honeywell	07/23/2007	16:55:35	entered geofence TSI updated
TEAMS_17092	Honeywell	07/23/2007	16:53:41	exited geofence TSI updated
TEAMS_17115	Cyanco	07/23/2007	16:50:42	position report event created
TEAMS_17086	Honeywell	07/23/2007	16:37:31	exited geofence TSI updated
TEAMS_17090	Honeywell	07/23/2007	16:31:04	entered geofence TSI updated
TEAMS_17091	Honeywell	07/23/2007	16:20:25	entered geofence TSI updated
TEAMS_17091	Honeywell	07/23/2007	16:18:05	entered geofence TSI updated
TEAMS_17092	Honeywell	07/23/2007	15:53:24	exited geofence TSI updated
TEAMS_10662	Honeywell	07/23/2007	15:50:59	exited geofence TSI updated
TEAMS_17089	Honeywell	07/23/2007	15:42:55	entered geofence TSI updated
TEAMS_17086	Honeywell	07/23/2007	15:37:14	exited geofence TSI updated
TEAMS_17079	Honeywell	07/23/2007	15:13:42	entered geofence TSI updated

into the TEAMS data base such as a telephone call. The Action Log View lists the ID of the event, the TEAMS username of the creator of the entry, the date and time entered, and the text of the action entry. The event ID displayed in the list is a hyperlink and by clicking on this link a user will navigate to the Event Details page for that event. Also displayed on the Action Log View page are tabs that a user can click on to navigate to the List View page, Map View page, or Emulator page.

1.9.4 The action log details page provides detailed information for actions related to individual shipments.

The TEAMS Action Log Details page illustrated in **Figure 1.12** shows all of the Action Log data for only the event whose details are currently being viewed. This page contains a table that shows all of the Action Log entries for this event. Each entry in the table includes the name of the person or system that created the entry, the date and time of the entry, and the actual Action Log entry text.

Figure 1.12 TEAMS action log details page



Event Action Log

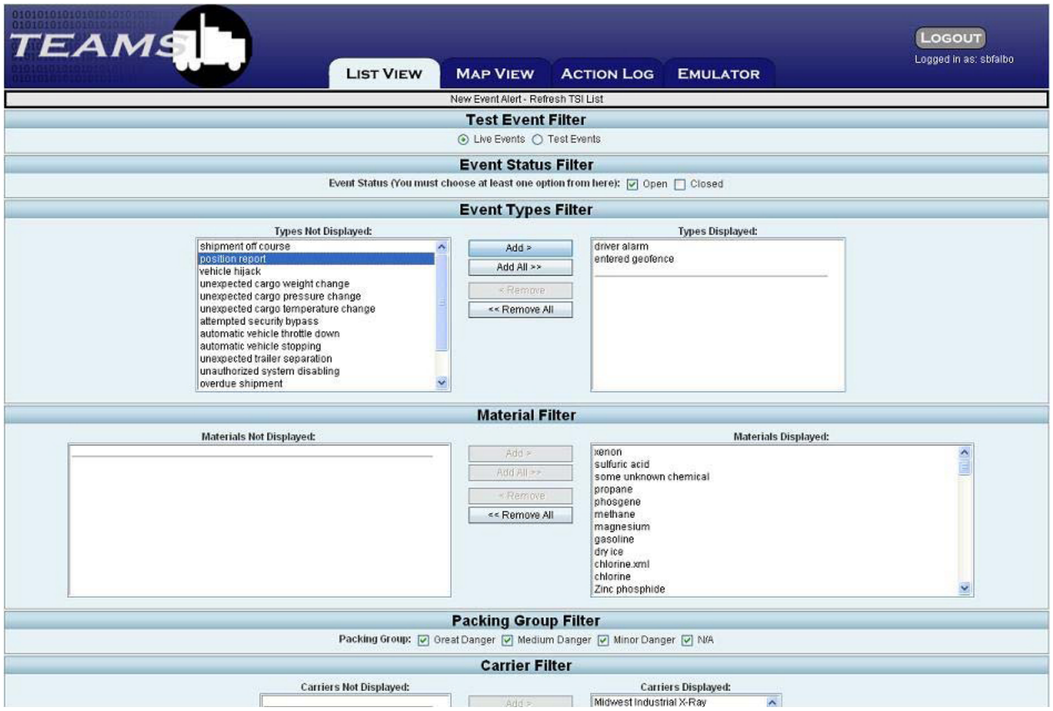
Creator	Date	Time	Action Item
sfalbo	07/23/2007	18:27:59	Cleared alert: entered geofence
sfalbo	07/23/2007	18:25:11	Called Tonawanda Police Department
sfalbo	07/23/2007	18:24:11	Called CompanyB
sfalbo	07/23/2007	18:23:59	Called TSA Watch Officer
sfalbo	07/23/2007	18:10:34	Event acknowledged
emulator	07/23/2007	18:05:02	entered geofence event created

1.9.5 Information on active shipments can be sorted and viewed using the event filters page.

The Event Filters page illustrated in **Figure 1.13** allows a TEAMS user to filter the events that are currently being displayed by TEAMS. The Event Filters page contains a radio button control allowing a user to choose whether to display live events or test events, a checkbox control that filters the display to show either open events, closed events, or both, and a checkbox control that filters based on the Packing Group of chemicals. Also included are multiple selection lists that allow the user to filter on Event Types, Materials, and Carriers. When the filters are modified, the List View, Map View, and Action Log View pages all reflect the filter options. From the Event Filters page, the user can also navigate to the Map View page, Action Log View page, or Emulator page using the tabs at the top of the page.

The events detail page allows users to prioritize the list view to display high priority events or events with a high risk rating.

Figure 1.13 TEAMS event filters page.



New Event Alert - Refresh TSI List

Test Event Filter

● Live Events ○ Test Events

Event Status Filter

Event Status (You must choose at least one option from here): ☑ Open □ Closed

Event Types Filter

Types Not Displayed:

shipment off course
position report
vehicle hijack
unexpected cargo weight change
unexpected cargo pressure change
unexpected cargo temperature change
attempted security bypass
automatic vehicle throttle down
automatic vehicle stopping
unexpected trailer separation
unauthorized system disabling
overdue shipment

Types Displayed:

driver alarm
entered geofence

Material Filter

Materials Not Displayed:

Materials Displayed:

xenon
sulfuric acid
some unknown chemical
propane
phosgene
methane
magnesium
gasoline
dry ice
chlorine.xml
chlorine
Zinc phosphide

Packing Group Filter

Packing Group: ☑ Great Danger ☑ Medium Danger ☑ Minor Danger ☑ N/A

Carrier Filter

Carriers Not Displayed:

Carriers Displayed:

Midwest Industrial X-Ray

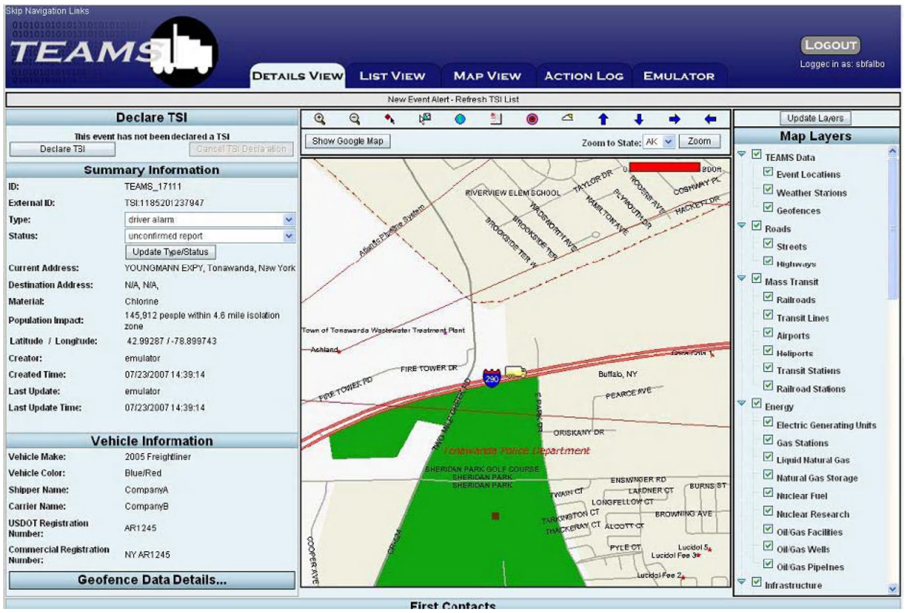
1.9.6 The event details page provides detailed information on individual shipments.

The Event Details page illustrated in **Figure 1.14** contains detailed information about a specific event in the TEAMS system. The Event Details page can be navigated to from either the List View page, the Map View page, or the Action Log View page. The Event Details page contains a map displaying the location of the vehicle, map navigation tools, and map overlay controls that allow a user turn map layers on and off as desired. The

The events details page provides detailed information on individual shipments.

Event Details page provides the ability for users with the proper permissions to declare the event a Transportation Security Incident (TSI) if instructed by TSA. Summary Information on the Event Details page includes the TEAMS ID of the event, the sending source's ID of the event, the event type and status, the address, the destination, the material being carried, the estimated population impact, the latitude/longitude location, the creator of the event, the time the event was created, the time of the event's most recent update, and who last updated the event. The event type and status can be updated by the TEAMS user in this section of the Event Details page. The Vehicle Information section displays the make and color of the vehicle, the shipper's name, the carrier's name, the USDOT registration number, and the commercial registration number. The Geo-fence Data Details section shows the names of the geo-fences being violated by this event and it also provides the ability for a TEAMS user to create a geo-fence that will 'track' the event being displayed.

Figure 1.14 TEAMS events details page.



Logged in as: sbfalbo

Declare TSI

This event has not been declared a TSI

Declare TSI | Cancel TSI Declaration

Summary Information

ID:	TEAMS_17111
External ID:	TSI:1185201237947
Type:	driver alarm
Status:	unconfirmed report
Current Address:	YOUNGMANN EXPY, Tonawanda, New York
Destination Address:	N/A, N/A,
Material:	Chlorine
Population Impact:	145,912 people within 4.6 mile isolation zone
Latitude / Longitude:	42.99287 / -78.899743
Creator:	emulator
Created Time:	07/23/2007 14:39:14
Last Update:	emulator
Last Update Time:	07/23/2007 14:39:14

Update Type/Status

Vehicle Information

Vehicle Make:	2005 Freightliner
Vehicle Color:	Blue/Red
Shipper Name:	CompanyA
Carrier Name:	CompanyB
USDOT Registration Number:	AR1245
Commercial Registration Number:	NY AR1245

Map Layers

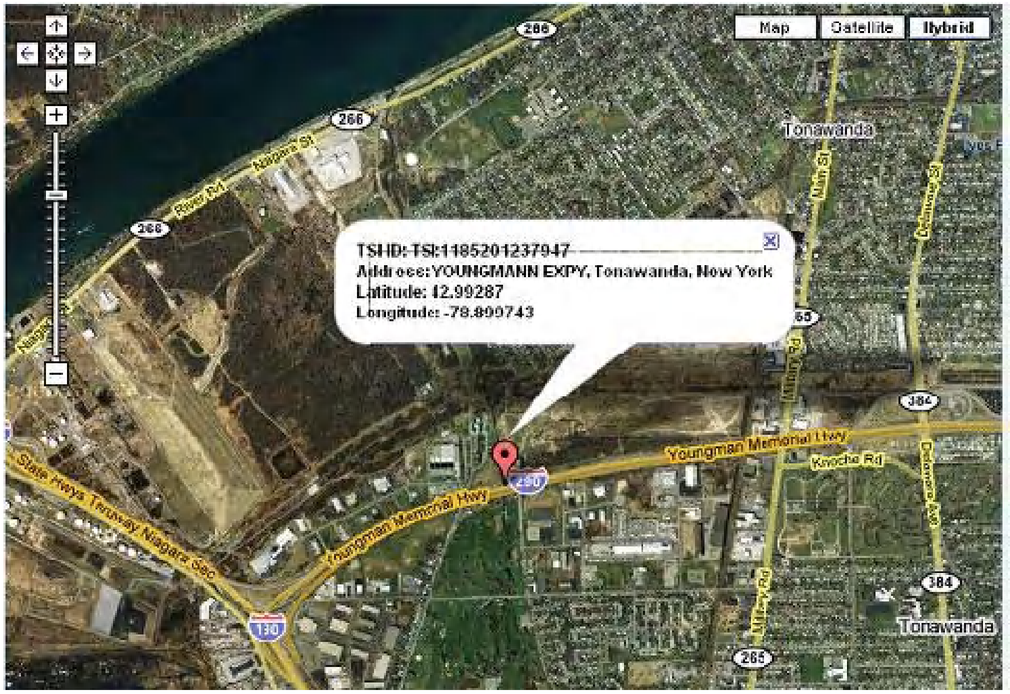
- ☑ TEAMS Data
  - ☑ Event Locations
  - ☑ Weather Stations
  - ☑ Geofences
- ☑ Roads
  - ☑ Streets
  - ☑ Highways
- ☑ Mass Transit
  - ☑ Railroads
  - ☑ Transit Lines
  - ☑ Airports
  - ☑ Heliports
  - ☑ Transit Stations
  - ☑ Railroad Stations
- ☑ Energy
  - ☑ Electric Generating Units
  - ☑ Gas Stations
  - ☑ Liquid Natural Gas
  - ☑ Natural Gas Storage
  - ☑ Nuclear Fuel
  - ☑ Nuclear Research
  - ☑ Oil/Gas Facilities
  - ☑ Oil/Gas Wells
  - ☑ Oil/Gas Pipelnes
- ☑ Infrastructure

The Google map page allows users to superimpose shipment data on a Google map and to use Google map controls.

1.9.7 The Google map superimposes vehicle location/data on Google maps.

The Google Map page illustrated in **Figure 1.15** is available by clicking on the 'Show Google Map' button in the map control section of the Event Details page. Clicking this button will open a secondary window that shows the truck's location along with overview data on a Google map (Figure 12). This page includes map controls to zoom in, zoom out, and pan as well as the ability to turn on orthographic map imagery.

Figure 1.15 TEAMS Google map page



TSI ID: TSI:1185201237947
Address: YOUNGMANN EXPY, Tonawanda, New York
Latitude: 42.99287
Longitude: -78.899743

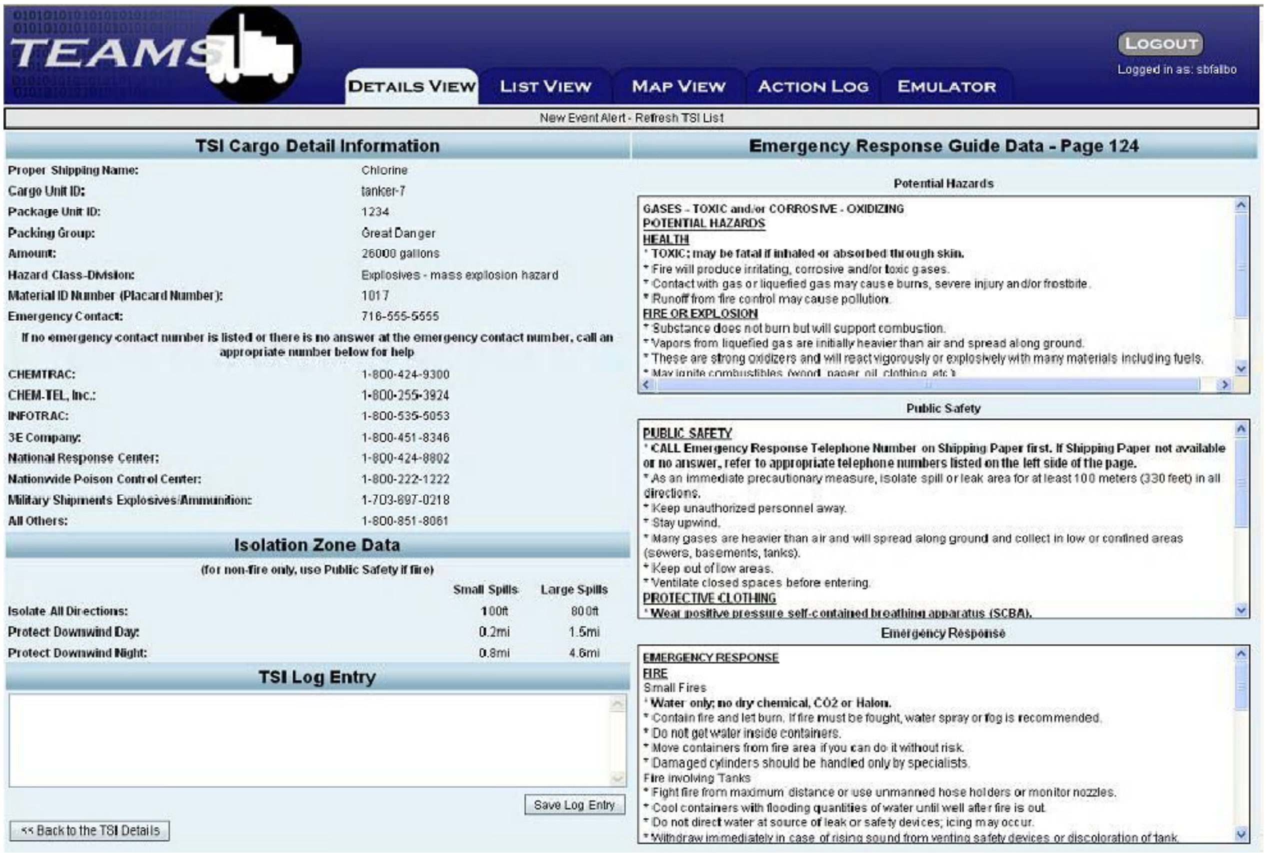
1.9.8 The cargo details page provided information on the type and quantity of materials on a carrier's vehicle.

The Cargo Details page illustrated in **Figure 1.16** displays information about the materials being transported during a shipment. Specific information about the material includes the proper shipping name of the material, the cargo unit ID, the package ID, the packing group, amount being transported, the hazard class and division, the material's United Nations (UN) number, and an emergency contact telephone number. The Cargo Details page also displays a list of numbers that can be called in no emergency contact telephone number is provided. These numbers include CHEMTRAC, CHEM-TEL, INFOTRAC, 3E Company, National Response Center, National Poison Control Center, Military Shipments Explosives/Ammunition, and a general number if none of the other numbers are appropriate.

The Cargo Details page displays information about the materials being transported during a shipment.

2004 Emergency Response Guide data related to the material is also available on the Cargo Details page. This includes Isolation Zone distance data and the actual guide page data from the Emergency Response Guide. The guide page data is broken up into three sections: Potential Hazards, Public Safety, and Emergency Response. A TEAMS user may also enter an entry into the Action Log using a textbox on the Cargo Details page.

Figure 1.16 TEAMS cargo details page.



TSI Cargo Detail Information

Proper Shipping Name:	Chlorine
Cargo Unit ID:	tanker-7
Package Unit ID:	1234
Packing Group:	Great Danger
Amount:	26000 gallons
Hazard Class-Division:	Explosives - mass explosion hazard
Material ID Number (Placard Number):	1017
Emergency Contact:	716-555-5555

If no emergency contact number is listed or there is no answer at the emergency contact number, call an appropriate number below for help

CHEMTRAC:	1-800-424-9300
CHEM-TEL, Inc.:	1-800-255-3924
INFOTRAC:	1-800-535-5053
3E Company:	1-800-451-8346
National Response Center:	1-800-424-8802
Nationwide Poison Control Center:	1-800-222-1222
Military Shipments Explosives/Ammunition:	1-703-697-0218
All Others:	1-800-851-8061

Isolation Zone Data

(for non-fire only, use Public Safety if fire)

	Small Spills	Large Spills
Isolate All Directions:	100ft	800ft
Protect Downwind Day:	0.2mi	1.5mi
Protect Downwind Night:	0.8mi	4.6mi

TSI Log Entry

Emergency Response Guide Data - Page 124

Potential Hazards

GASES - TOXIC and/or CORROSIVE - OXIDIZING
POTENTIAL HAZARDS
HEALTH
* **TOXIC; may be fatal if inhaled or absorbed through skin.**
* Fire will produce irritating, corrosive and/or toxic gases.
* Contact with gas or liquefied gas may cause burns, severe injury and/or frostbite.
* Runoff from fire control may cause pollution.
FIRE OR EXPLOSION
* Substance does not burn but will support combustion.
* Vapors from liquefied gas are initially heavier than air and spread along ground.
* These are strong oxidizers and will react vigorously or explosively with many materials including fuels.
* May ignite combustibles (wood, paper, oil, clothing, etc.).

Public Safety

PUBLIC SAFETY
* **CALL Emergency Response Telephone Number on Shipping Paper first. If Shipping Paper not available or no answer, refer to appropriate telephone numbers listed on the left side of the page.**
* As an immediate precautionary measure, isolate spill or leak area for at least 100 meters (330 feet) in all directions.
* Keep unauthorized personnel away.
* Stay upwind.
* Many gases are heavier than air and will spread along ground and collect in low or confined areas (sewers, basements, tanks).
* Keep out of low areas.
* Ventilate closed spaces before entering.
PROTECTIVE CLOTHING
* **Wear positive pressure self-contained breathing apparatus (SCBA).**

Emergency Response

EMERGENCY RESPONSE
FIRE
Small Fires
* **Water only; no dry chemical, CO2 or Halon.**
* Contain fire and let burn. If fire must be fought, water spray or fog is recommended.
* Do not get water inside containers.
* Move containers from fire area if you can do it without risk.
* Damaged cylinders should be handled only by specialists.
Fire involving Tanks
* Fight fire from maximum distance or use unmanned hose holders or monitor nozzles.
* Cool containers with flooding quantities of water until well after fire is out.
* Do not direct water at source of leak or safety devices; icing may occur.
* Withdraw immediately in case of rising sound from venting safety devices or discoloration of tank.

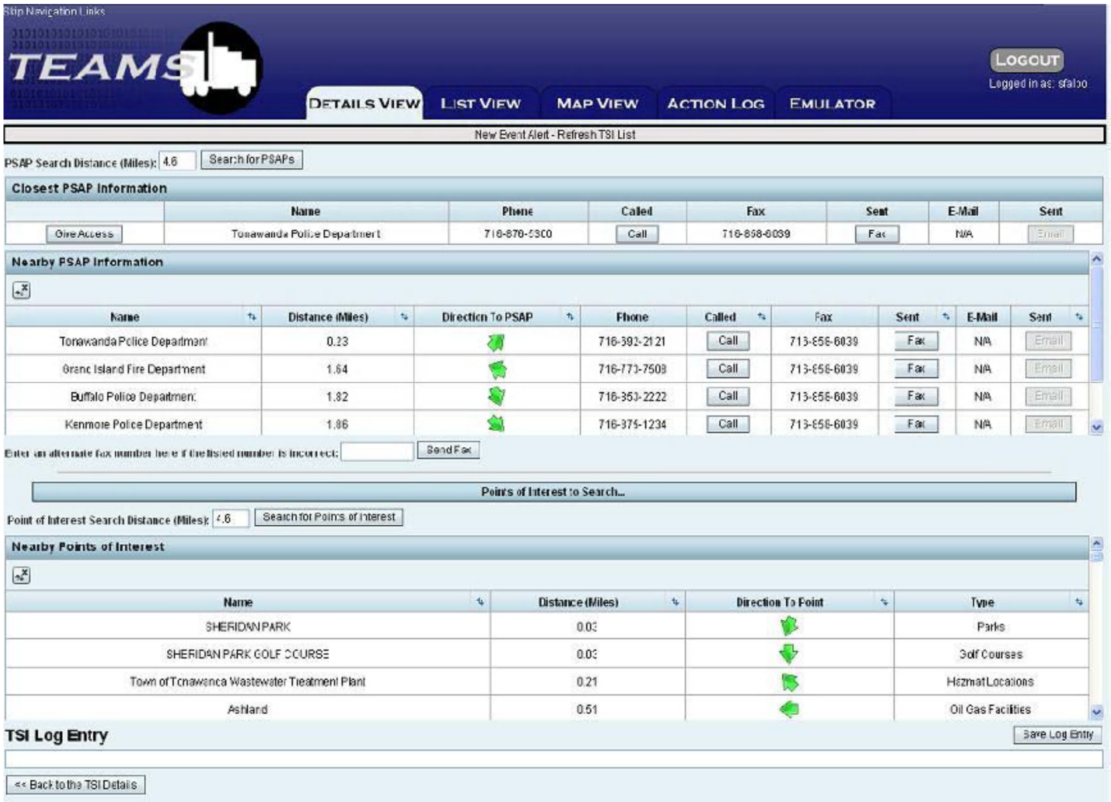
1.9.9 The PSAP/points of interest page displays vehicles and points of interest on a map.

TEAMS was designed with the idea that a Public Sector Answering Point (PSAP) would be the government action agency that would manage the response to hazmat incidents. For the HTSP, the HTSP contractor used a medical dispatch center in the Buffalo metropolitan area as the monitoring point for HTSP systems. The assumption during the pilot program is that local PSAPs, like the medical dispatch center, would be the government action agency that would coordinate on-scene response activities when a hazmat incident occurred.

The HTSP uses local city/county agencies (PSAPs) as the contact points for hazmat incidents. The nearest PSAP is identified on the map when there is an incident.

The PSAP/Points of Interest Details View illustrated in **Figure 1.17** displays information about the PSAPs and Points of Interest that are within the proximity of the shipment's location. Contact information for the PSAP whose region this shipment is currently located within is always displayed in the first table on this page. TEAMS users can also search for PSAPs near the shipment by entering a search radius in a textbox on the page. The search results will populate a table that will display the contact information for all of the PSAPs contained within the entered radius. These search results include the name of the PSAP, its phone number, fax number, email address, distance to the PSAP, and its direction in relation to the location of the shipment. Each entry in the table includes buttons to add entries to the Action Log either indicating that a phone call was placed to the PSAP or an email sent to the PSAP along with a button that will send a fax of summary information to the PSAP. After the table is a textbox that a TEAMS user can use to send a summary information fax to a PSAP whose number may not be listed.

Figure 1.17 TEAMS points of interest page.



PSAP Search Distance (Miles): 4.6 [Search for PSAPs]

Closest PSAP Information

	Name	Phone	Called	Fax	Sent	E-Mail	Sent
Give Access	Tonawanda Police Department	716-878-5300	Call	716-858-6039	Fax	N/A	Email

Nearby PSAP Information

Name	Distance (Miles)	Direction To PSAP	Phone	Called	Fax	Sent	E-Mail	Sent
Tonawanda Police Department	0.23	↗	716-392-2121	Call	713-858-6039	Fax	N/A	Email
Granc Island Fire Department	1.64	↖	716-773-7508	Call	713-858-6039	Fax	N/A	Email
Buffalo Police Department	1.82	↓	716-353-2222	Call	713-858-6039	Fax	N/A	Email
Kenmore Police Department	1.86	↘	716-375-1234	Call	713-858-6039	Fax	N/A	Email

Enter an alternate fax number here if the listed number is incorrect: [Send Fax]

Points of Interest to Search...

Point of Interest Search Distance (Miles): 4.6 [Search for Points of Interest]

Nearby Points of Interest

Name	Distance (Miles)	Direction To Point	Type
SHERIDAN PARK	0.03	↑	Parks
SHERIDAN PARK GOLF COURSE	0.03	↓	Golf Courses
Town of Tonawanda Wastewater Treatment Plant	0.21	↖	Hazmat Locations
Ashland	0.51	←	Oil Gas Facilities

TSI Log Entry [Save Log Entry]

[<< Back to the TSI Details]

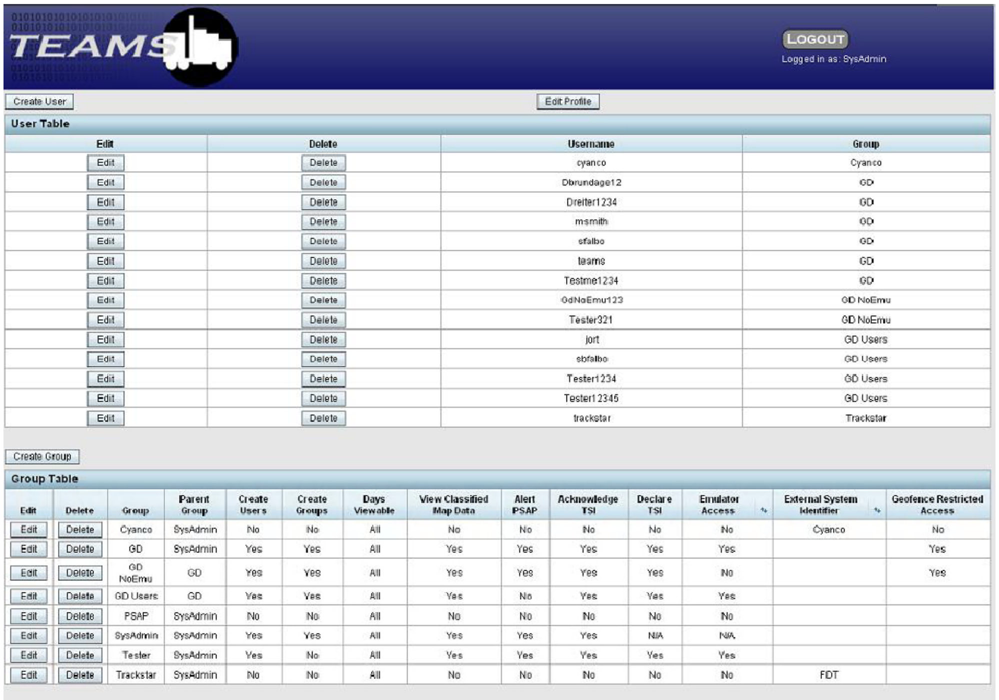
This page is also used to display any Points of Interest that are near the shipment's current location. A TEAMS user can search for Points of Interest near the shipment by entering a search radius in another textbox on the page. After entering the search radius, the TEAMS user then selects which map overlays to search from a multiple selection list that shows the names of all of the searchable layers. Once the user has selected the desired layers to search, a button must be clicked to conduct the search. The search results are displayed in a table that lists the name of the Point of Interest, the name of the layer containing the Point of Interest, its distance from the shipment, and its direction in relative to the shipment's location. A TEAMS user may also enter an entry into the Action Log using a textbox on the PSAP/Points of Interest Details page.

The user rights page displays user rights that have been assigned to individuals by system administrators.

1.9.10 The user management page lets system administrators assign and manage user rights.

The initial page of the User Management module illustrated in **Figure 1.18** is the Overview page. This page contains an 'Edit Profile' button for all logged in users. This button will allow the user to navigate to a page that will allow the user to update profile information. If the user has the appropriate privileges, the 'Create User' and 'Create Group' buttons will be shown which will allow for navigation to the respective pages. Also, two tables will be displayed that show all of the users and groups that the logged in user can administer. The user table contains the username of each user, its group affiliation, an edit button, and a delete button. The group table contains the name of each group, its parent group, an edit button, a delete button, and various properties that are used to restrict the group's permissions within the TEAMS application. The properties displayed for each group are Create Users, Create Groups, View Classified Map Data, Alert PSAP, Acknowledge TSI, Declare TSI, Emulator Access, External System Identifier, and Geo-fence Restricted Access.

Figure 1.18 TEAMS user management page.



User Table

Edit	Delete	Username	Group
Edit	Delete	cyanco	Cyanco
Edit	Delete	Dbrundage12	GD
Edit	Delete	Dreiter1234	GD
Edit	Delete	msmith	GD
Edit	Delete	sfalbo	GD
Edit	Delete	teams	GD
Edit	Delete	Testme1234	GD
Edit	Delete	GdNoEmu123	GD NoEmu
Edit	Delete	Tester321	GD NoEmu
Edit	Delete	jort	GD Users
Edit	Delete	sbfalbo	GD Users
Edit	Delete	Tester1234	GD Users
Edit	Delete	Tester1 2345	GD Users
Edit	Delete	trackstar	Trackstar

Group Table

Edit	Delete	Group	Parent Group	Create Users	Create Groups	Days Viewable	View Classified Map Data	Alert PSAP	Acknowledge TSI	Declare TSI	Emulator Access	External System Identifier	Geofence Restricted Access
Edit	Delete	Cyanco	SysAdmin	No	No	All	No	No	No	No	No	Cyanco	No
Edit	Delete	GD	SysAdmin	Yes	Yes	All	Yes	Yes	Yes	Yes	Yes		Yes
Edit	Delete	GD NoEmu	GD	Yes	Yes	All	Yes	Yes	Yes	Yes	No		Yes
Edit	Delete	GD Users	GD	Yes	Yes	All	Yes	No	Yes	Yes	Yes		
Edit	Delete	PSAP	SysAdmin	No	No	All	No	No	No	No	No		
Edit	Delete	SysAdmin	SysAdmin	Yes	Yes	All	Yes	Yes	Yes	N/A	N/A		
Edit	Delete	Tester	SysAdmin	Yes	No	All	Yes	Yes	Yes	Yes	Yes		
Edit	Delete	Trackstar	SysAdmin	No	No	All	No	No	No	No	No	FDT	

1.10 TEAMS allows users to build and manage geo-fences.

Initially the geo-fence solution in the HTSP prototype only allowed a user to create a geo-fence around an existing transportation event in the TEAMS. This geo-fence's location would update whenever there was a position update to the event that the geo-fence was created around. Whenever another transportation event entered the boundary of the geo-fence, the event's type would be changed to 'entered geo-fence' and the TEAMS operators would be alerted that an event had entered a geo-fence.

Initially, the HTSP prototype only allowed geo-fences to be built around an active event. For example, a geo-fence was built around a truck and when it got within a certain distance of a vulnerable object, the system registered a geo-fence event.

As more trucks were added to the TEAMS system, the need for a more full featured geo-fencing capability emerged and the geo-fencing feature was re-designed. This new design allowed TEAMS operators to create geo-fences in multiple ways using a set of Geo-fence Designer web pages. Users could create free-form geo-fences by drawing shapes on a map, they could upload an existing ESRI shape-file from their hard drive, or they could select geographic features from the existing ESRI shape-files.

Also included in the geo-fence redesign was a new method of assigning violation distances to geo-fences. Previously, it was thought that the user would create a geo-fence region and then add various proximity levels to the geo-fence to determine violations. Consider the following case: a user would create a geo-fence around the Pentagon and then assign multiple buffer distances to the shape. Trucks carrying phosgene would be required to remain 10 miles away from the Pentagon while trucks carrying gasoline would be required to remain 1/2 mile from the Pentagon. This process would have to occur for each chemical. This becomes a maintenance issue rather quickly as multiple geo-fences are created. The HTPS contractor addressed this problem by allowing the TEAMS operator to create a single shape for the geo-fence without

New geo-fence authoring tools and a new approach to geo-fence maintenance were added to the prototype by the HTSP contractor.

creating various distance buffers around the geo-fence. Instead, these distance buffers are determined by each truck on an individual basis. Each truck carrying a chemical has a buffer that is determined by the Emergency Response Guide isolation zone distance specified for the chemicals on the truck. Geo-fence violations occur when this isolation zone distance buffer crosses the boundary of a geo-fence created by a TEAMS user.

The effectiveness of the geo-fence approach developed by the HTSP contractor is a function of vehicle location reporting frequency. If the frequency is too low, the geo-fencing approach will not work well.

An issue that was still remaining with this approach is the overall usefulness of geo-fencing when position reports are received at long time intervals. Assuming that most trucks will report every hour, it is possible that a truck may pass through a geo-fence without a TEAMS operator every being made aware that a geo-fence violation occurred. Our approach to lessening the impact of this issue was to add a second buffer distance around each truck that takes into account the reporting interval of the truck. A geo-fence violation is generated when this second buffer is violated just as it is when the smaller buffer distance is violated. The formula for computing the second buffer distance is: isolation zone distance + (reporting interval * speed). The reporting interval variable is determined dynamically by taking the average time between the last five messages received regarding the truck and speed is assumed to be 60 miles per hour.

Geo-fences can be programmed with different properties. They may be exclusionary (a violation when a truck enters the geo-zone) or inclusionary (a violation when a truck leaves the geo-zone).

Various properties can also be assigned to Geo-fences as they are created. Geo-fences can be assigned a start time and an end time to establish the time period for which they are active. Geofences can also have a list of chemicals assigned to them designating that only trucks carrying these specified chemicals will create a geo-fence alert upon a boundary violation. Also, geofences are either classified as exclusionary zones or inclusionary zones. An exclusionary zone creates a violation when an event enters its geographic boundary. Conversely, inclusionary zones generate a violation when an event exits the boundary established by the inclusionary zone. An inclusionary zone must have events 'assigned' to it and it is only for these events that an inclusionary zone will generate an alert upon violation of the boundary. Inclusionary zones can best be thought of as a manner of introducing route adherence to TEAMS.

The revised approach to creating and managing geo-fences has been successful in adding a more full featured set of tools to TEAMS. Creating a separate set of pages that allow for the management of geo-fences is more flexible and useful to the TEAMS operators than just allowing users to create a geo-fence at an existing event's location.

The geo-fence approach used in the HTSP pilot will create false alarms – possibly an overwhelming number of false alarms for the truck tracking center.

The amount of geo-fence management time required by the TEAMS users was a concern when creating the geo-fence feature. The approach of using the isolation zone distance assigned to the truck rather than assigning various buffer distances to each geo-fence has removed much of the burden associated with creating geo-fences. The users of the TEAMS geo-fence module only have to define the geographic area of interest and the TEAMS software is responsible for determining all of the violations dynamically for each truck. This removes much of the burden from the TEAMS operators.

The usefulness of the geo-fencing feature is contingent on the reporting intervals of the trucks. By creating a second ring around the truck's location, we are able to detect more geo-fence violations but subsequently, more false alarms are created.

The HTSP prototype has a number of linked pages for geo-fence management.

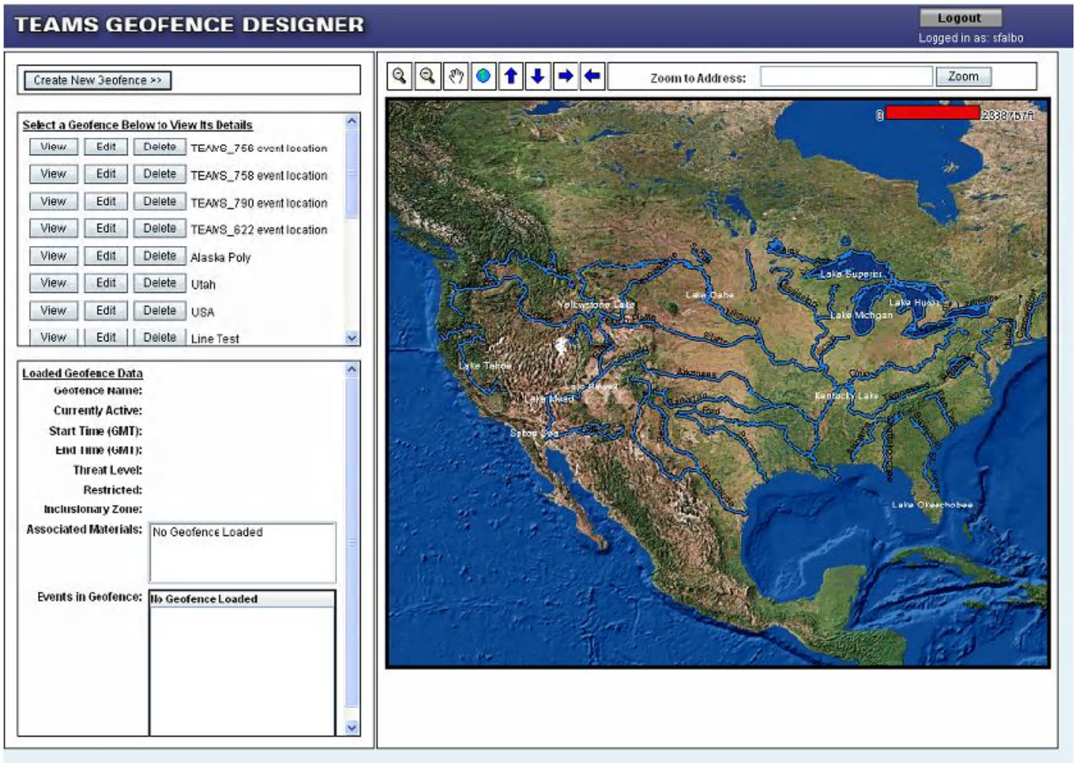
1.10.1 The HTSP prototype has a number of linked pages for geo-fence management.

As illustrated in **Figure 1.8**, TEAMS has a number of linked pages for geo-fence management. The geo-fence management overview page, illustrated in **Figure 1.19**, has a 'Create New Geo-fence' button that will let a user create a new geo-fence. This page also contains a list of the names of all geo-fences that have been created. For each geo-fence listed there are buttons to view, edit, or delete the geo-fence. Clicking on the 'View' button next to a geo-fence's name will load the geo-fence's details on the overview page. The map portion of the page will update to show the location of the geo-fence as well as the locations of all of the events that are violating the geo-fence's geographic boundary. The map portion contains controls that allow the user to zoom in, zoom out, pan, and navigate to an address entered by the user.

The geo-fence general information page allows users to enter baseline data on geo-fences they want the system to monitor.

Other geo-fence details are displayed in a table in the lower left hand portion of this page. These details include the geo-fence's name, whether or not it is currently active, start time, end time, threat level, whether or not it has restricted access, if it is an inclusionary zone, and its associated materials. Also included in this table is an

Figure 1.19 TEAMS geo-fence management overview page.



'accordion' style component that lists the details of the events that have violated the geo-fence. Each pane in the 'accordion' component has the title bar set to the event's TEAMS ID and the text in each pane lists the address, event type, material, and population impact of the event. Clicking on an 'Edit' button will take the user to the Edit Geo-fence page for that geo-fence.

1.10.2 The general information page lets users enter basic data about geo-fences they create.

The Geo-fence General Information page, illustrated **in Figure 1.20**. lets a user enter general details about a geo-fence that is being created. The user must enter a unique name for the geo-fence in the text field on the page. An optional start time and/or end time may be entered using calendar controls on the page as well. Radio button groups are provided to enter the geo-fence's threat level, restricted status, and type. There are also fields that will allow users to specify events to associate with the geo-fence, assign materials to the geo-fence, and choose the method for creating the geo-fence. If associated events are to be specified, the user will enter this information on the Geo-fence Associated Event page. Presently, the only supported option for creating the geo-fence is 'Free-form Map Drawing' but in the future map overlay points of interest selection and shape file uploading will provide additional options for geo-fence creation.

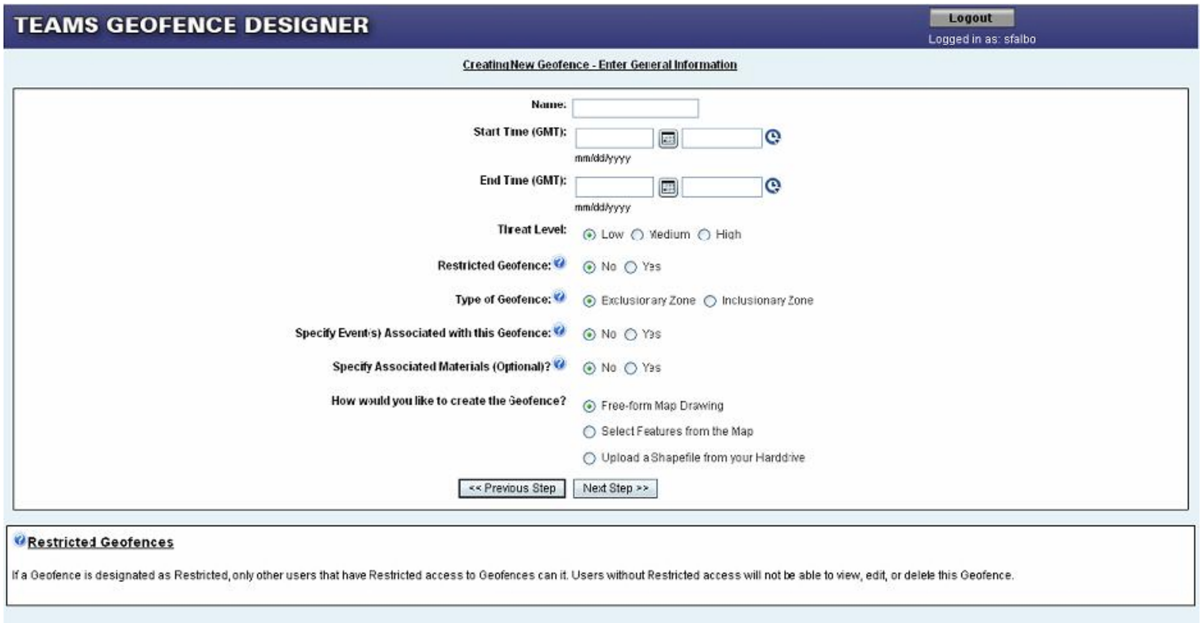
There is also a dynamic help box on the page that the user can use to get help about specific geo-fence properties that may not be straight-forward. The user can click on any of the question mark icons next to a property label to change the information shown in the help box.

1.10.3 The geo-fence associated event page lets users associate events with geo-fences.

The associate event page lets users link a geo-fence with individual shipments.

The Geo-fence Associated Event page, illustrated in **Figure 1.21**, contains a list that allows the user to select an event or events to associate with an event in the TEAMS

Figure 1.20 TEAMS geo-fence general information page



TEAMS GEOFENCE DESIGNER

Logout

Logged in as: sfalbo

Creating New Geofence - Enter General Information

Name:

Start Time (GMT): mm/dd/yyyy

End Time (GMT): mm/dd/yyyy

Threat Level: ● Low ○ Medium ○ High

Restricted Geofence: ● No ○ Yes

Type of Geofence: ● Exclusionary Zone ○ Inclusionary Zone

Specify Event(s) Associated with this Geofence: ● No ○ Yes

Specify Associated Materials (Optional)? ● No ○ Yes

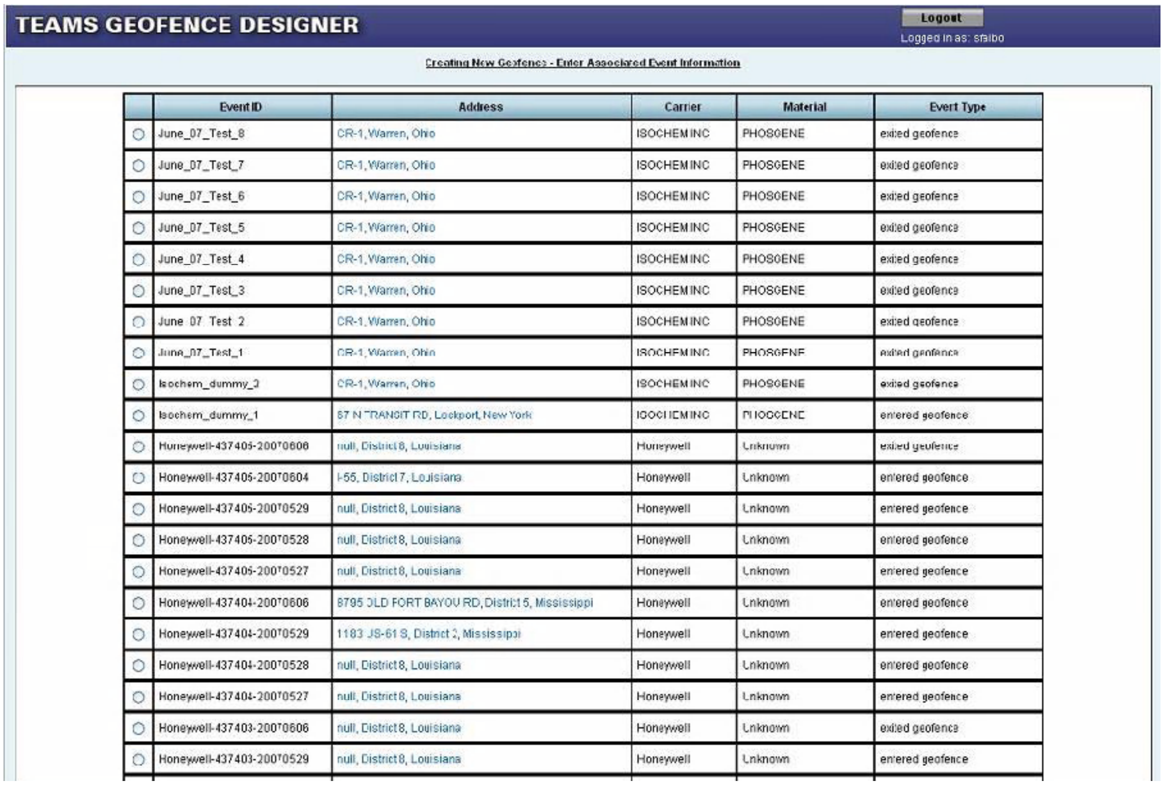
How would you like to create the Geofence? ● Free-form Map Drawing ○ Select Features from the Map ○ Upload a Shapefile from your Harddrive

<< Previous Step | Next Step >>

Restricted Geofences

If a Geofence is designated as Restricted, only other users that have Restricted access to Geofences can it. Users without Restricted access will not be able to view, edit, or delete this Geofence.

Figure 1.21 Geo-fence associated event page



TEAMS GEOFENCE DESIGNER

Logout

Logged in as: sfalbo

Creating New Geofence - Enter Associated Event Information

	Event ID	Address	Carrier	Material	Event Type
○	June_07_Test_8	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_7	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_6	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_5	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_4	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_3	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_2	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	June_07_Test_1	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	Isochem_dummy_2	CR-1, Warren, Ohio	ISOCHEM INC	PHOSGENE	exited geofence
○	Isochem_dummy_1	67 N TRANSIT RD, Lockport, New York	ISOCHEM INC	PHOSGENE	entered geofence
○	Honeywell-437406-20070606	null, District 8, Louisiana	Honeywell	Unknown	exited geofence
○	Honeywell-437406-20070604	I-55, District 7, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437406-20070529	null, District 8, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437406-20070528	null, District 8, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437406-20070527	null, District 8, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437404-20070606	8795 OLD FORT BAYOU RD, District 5, Mississippi	Honeywell	Unknown	entered geofence
○	Honeywell-437404-20070529	1183 US-61 S, District 2, Mississippi	Honeywell	Unknown	entered geofence
○	Honeywell-437404-20070528	null, District 8, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437404-20070527	null, District 8, Louisiana	Honeywell	Unknown	entered geofence
○	Honeywell-437403-20070606	null, District 8, Louisiana	Honeywell	Unknown	exited geofence
○	Honeywell-437403-20070529	null, District 8, Louisiana	Honeywell	Unknown	entered geofence

system. Exclusionary zones can only have one event associated with them while Inclusionary zones must have at least one or more events associated with them. If an event is associated with an Exclusionary zone, there is no need to draw the geo-fence on a map since the geo-fence's location is the same as the location of the event. The event list contains the ID, address, carrier, material, and event type information for each non-test event active in TEAMS. The address is a link component that when clicked opens a popup window displaying a Google map of the event's location. If the geo-fence is an Exclusionary zone, each entry in the table contains a radio button allowing for the selection of one event only. If the geo-fence is an Inclusionary zone, each row in the table contains a checkbox component which will allow the user to select more than one event to associate with the geo-fence. Clicking on the 'Next Step' button on this page will create the geo-fence if it is an Exclusionary zone or navigate to the Geo-fence Creation Wizard Drawing page if it is an Inclusionary zone.

1.10.4 The geo-fence creation wizard drawing page lets users create the geographic boundary of a geo-fence.

The Geo-fence Creation Wizard Drawing page, illustrated in **Figure 1.22**, provides the functionality for a user to create the geographic boundary of the geo-fence.

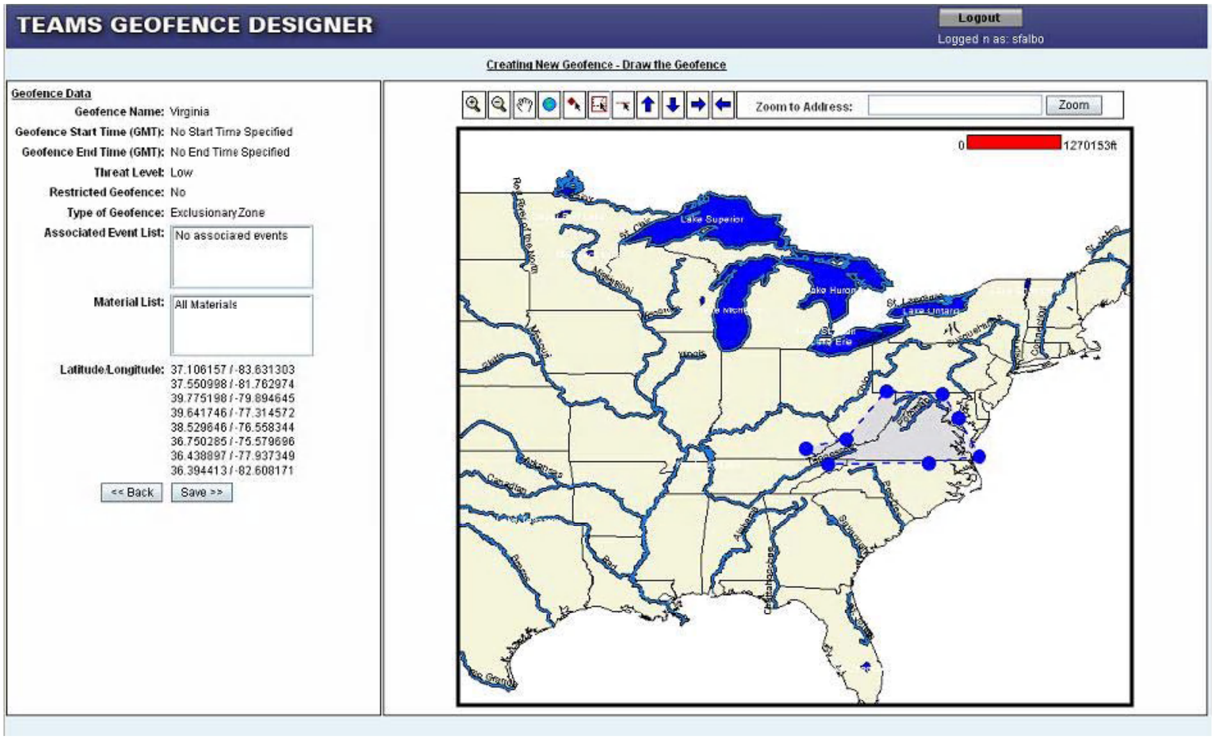
This page includes a column displaying the information about the geo-fence that the user has previously entered in the creation process. This information includes the geo-fence's name, start time, end time, threat level, restriction status, associated events, and associated material list.

A geo-fence drawing tool allows users to create the geographic boundary of a geo-fence.

There is also an area that dynamically displays the latitude and longitude location of points as they are added to the geo-fence. The 'Back' button allows the user to return to a previous page to edit any of the information they have previously entered.

This page also has a map component on which the user will draw the geo-fence. The map component contains standard navigation tools such as zoom in, zoom out, zoom to an address, and pan but it also contains three tools allowing a user to draw the geo-fence on the map. These tools are draw point, draw line, and draw polygon for each of the three types of geo-fence shapes that may be created. Once the user has used one of these map tools to draw the geo-fence, the 'Save' button can be clicked to store the geo-fence and compute any violations with existing events.

Figure 1.22 TEAMS geo-fence creation wizard drawing page



Geofence Data

Geofence Name: Virginia

Geofence Start Time (GMT): No Start Time Specified

Geofence End Time (GMT): No End Time Specified

Threat Level: Low

Restricted Geofence: No

Type of Geofence: ExclusionaryZone

Associated Event List: No associated events

Material List: All Materials

Latitude/Longitude:
37.106157 / -83.631303
37.550998 / -81.762974
39.775198 / -79.894645
39.641746 / -77.314572
38.529646 / -76.558344
36.750285 / -75.579696
36.438897 / -77.937349
36.394413 / -82.608171

1.11 A risk (business rules) engine was successfully demonstrated in the HTSP. [5]

The FDfolio™ software suite was used in the HSTP as a business rules engine to identify security risks in hazmat transportation.

The HTSP contractor was given the following direction from TSA.

> *"Assess the feasibility and benefits of a risk-based approach to filtering hazmat events and alerts on a prioritized basis in order to minimize false alarms and facilitate more timely identification of security threats."*

To address this directive, the contractor analyzed the feasibility of using the UCI and risk assessment analytic capability of the FDfolio™ software suite to supplement TEAMS in identifying hazmat security risks and distinguishing hazmat events that warrant enhanced monitoring and/or follow-up action from those that do not. [6]

The importance of distinguishing between hazmat events that warrant enhanced monitoring and / or follow-up action from those that do not is driven by the potentially large number of hazmat events that could represent security threats and the grave nature of the consequences of a security situation that is not detected. The goal of this task is therefore to explore how to eliminate HAZMAT events that are not security risks without labor-intensive scrutiny while not overlooking real security events.

The UCI and FDfolio™ were connected to feed data from hazmat shipments to the business (risk) rules engine in FDfolio™.

TEAMS was modified to present the results of risk-based analyses, and the UCI was used to connect to FDfolio™. These modifications included changes to each system to support: (1) the needed data sharing; and (2) changes within each system to implement the new functionality associated with risk assessment activities. Modifications to TEAMS included changes to the database to handle risk assessment specific data (i.e., risk level, risk description, recommendations for risk response, and the FDfolio™ URL to allow access to risk assessment details), and updates to displays to present risk-based alerts, risk assessment data, and recommendations. Finally, TEAMS was enhanced to implement the IEEE-1512 "WatchFor" message used to share risk assessment related information with FDfolio™.

FDfolio™ was also modified to support the TSA hazardous material truck tracking pilot. The primary custom component developed to accommodate data exchange and analysis

[5] c is taken from, "*Hazmat Truck Security Pilot – Final Report – Objective 4, Risk Assessment Feasibility Analysis";* April 11, 2008; General Dynamics Advanced Information Systems.

[6] FDfolio™ is a commercial software product offered by FreightDesk. At its heart is a business rules engine, and this component of the FDfolio™ product was used for risk-based shipment profiling the HTSP. The FDfolio™ product has many powerful features which were not used extensively in the pilot program. A description of the broad set of capabilities of FDfolio™ follows.

The "FDfolio™ Suite," provides a platform for implementing risk-based solutions for freight transportation security. Built into the suite are several risk assessment tools to support the analysis of risks (i.e., link analysis, data mining, predictive/probabilistic modeling, GIS spatial, and other analysis tools). FDfolio™ risk assessment involves four processing stages; data sourcing, data fusion, risk assessment, and risk output processing. Each of these process stages are summarized below.

- Data Sourcing – FDfolio™ employs a state-of-the-art multimodal data architecture organized around commercial freight transportation data and processes. The system is designed for efficient, high-volume data capture, validation, integration, and management. FDfolio™ enables data integrity and compliance checks on data sources and enables the aggregation of data from various and disparate sources. If messages are rejected for either syntax, compliance or data accuracy an error report will be generated and will provide the error codes and their reason. Error reports can be available online or can be incorporated in XML document, email or other types of electronic alerts. This information process flexibility enables easy collection of data from voluntary and/or private sector resources whose information are critical to enabling rich situational awareness.

- Data Fusion – FDFusion™ provides a "connect-the-dots" data repository that captures, reorganizes, and maintains a complete dataset of transactional, commercial, reference, activity, and status data on individual cargo movements (Rail, Maritime, Air, Surface, inter-modal). FDFusion™ is the engine that enables the capture, normalization and synthesis of disparate data to enable both a common operating picture and the basis for information analytics.

- Risk Assessment – FDAnaylzer maintains rule sets in a central/shareable repository, which promotes consistent decision-making. FDAnalyzer™ provides a user interface to enable analysts and other approved users to create and manage rules. FDAnalyzer™ empowers the users to create their own rules set as opposed to having to rely on technical support to write the rules. Risk scores are assigned to each transaction based on several factors that assign weights on both an absolute and relative risk-basis for the discovered threats and vulnerabilities, facilitating smoother prioritization of mitigation tasks. Several additional tools for analyzing and visualizing shipment information and HAZMAT related risks are also provided.

- Risk Based Output Processing – FDAnalyzer™ provides the interface for the user to monitor the outputs generated by the activated rules such as alerts on transactions that have triggered user-defined threshold requirements. FDAnalyzer™ presents transaction-based score results in a navigable drill-down interface, in which a shipment's total risk score is supported by a detailed risk-scoring matrix which is further supported by individual rule-based results. A reporting capability enables easy presentation of FDAnalyzer™ activities and results to other interested stakeholders. This capability is provided using a secure browser that can be accessed via TEAMS.

between the TEAMS system and the FDfolio™ risk analysis module was the UCI Data Exchange Interface (UCIDEI). The UCIDEI is a collection of web services and native folio "control agents" that support bidirectional data flow and data mapping. A custom application programming interface (API) used by the FDfolio™ rules is also packaged with the UCIDEI. The API is tailored specifically for the Truck Tracking Pilot rules and scenarios. FDfolio™ was also modified to support the process of obtaining data from carriers that do not support the UCI, other than for position reports. FDfolio™ was modified to support the generation of messages for key events including gate-out, gate-in, alerts, and position reports. These messages also contain information describing the truck and its cargo. For these carriers, FDfolio™ delivers outgoing UCI messages to TEAMS to indicate key hazmat shipment events such as gate-out or gate-in.

1.11.1 The UCI, TEAMS, and FDfolio™ interact to provide dynamic risk-based hazmat shipment tracking based on "events" as they occur.

Positioning the FDfolio™ product as the business rules engine for the HTSP prototype required an adjustment in the way the three main components of the system – the UCI, TEAMS, and FDfolio™ - worked together. The concept of operations also needed adjustment.

The HTPS system for risk assessment employs an event-driven architecture. Triggering events can occur at the carrier, truck, or truck tracking center, and are communicated directly to both TEAMS and FDfolio™ using the IEEE-1512 based Universal Communication Interface (UCI).

There are four types of triggering events:

1. Location update – The HAZMAT trucks generate location updates at specified intervals and are communicated to the HTSS. The system does not currently generate alerts when an expected update is not received, but this can be added.

2. Gate-out – When a HAZMAT truck first leaves the terminal with a load it issues a "gateout" indicating that the shipment has begun. In some cases, the first location report for a shipment serves as the gate-out message.

3. Gate-in – When a HAZMAT truck arrives at its destination a gate-in message is generated indicating that the shipment is complete. This is complicated in that HAZMAT trucks can have multiple destinations for a shipment and therefore can have several gate-ins.

4. Declared emergency – In addition to the routine messages associated with normal operations, a manually generated panic button message can be generated. Additional messages from the carrier or commercial truck tracking systems are also anticipated in the future such as hijacking, unexpected decoupling, missed gate-in, unexpected loss of weight or pressure, and etc.

Each new triggering event generates a new risk assessment. The risk assessments are conducted by TEAMS and FDfolio™ working together. TEAMS evaluates each truck location update to determine if there has been a geo-fence violation. If a geo-fence violation has occurred, TEAMS displays this and forwards a UCI message to FDfolio™ indicating the violation so the FDfolio™ can determine a risk level for the situation.

The risk profile of a hazmat shipment is changes as the truck moves. For example, when coming closer to more sensitive areas, the risk will rise. Alerts and events can also change the shipment profile. Dynamic risk profiling will be an important feature of the truck tracking center.

FDfolio™ receives all event messages from the commercial truck tracking systems as well as messages from TEAMS when geo-fence violations occur. FDfolio™ considers all information known about the shipment together with the information conveyed in the message to determine a risk level. Additionally, FDfolio™ considers historical information it has for the carrier based on past shipments and consults available TSA watch lists.

The risk level determined by FDfolio™ is sent to TEAMS for display and alerting. When risk level is high or severe TEAMS alerts Truck Tracking Center (TTC) operators and provides notification to the TTC Watch Officer. By considering all aspects of the shipment, historical data, TSA watch lists, and the current event and situation, the risk assessment approach attempts to minimize false alarms while enhancing the ability to

The data interaction within a truck tracking system enables watch officers to make timely decisions with confidence.

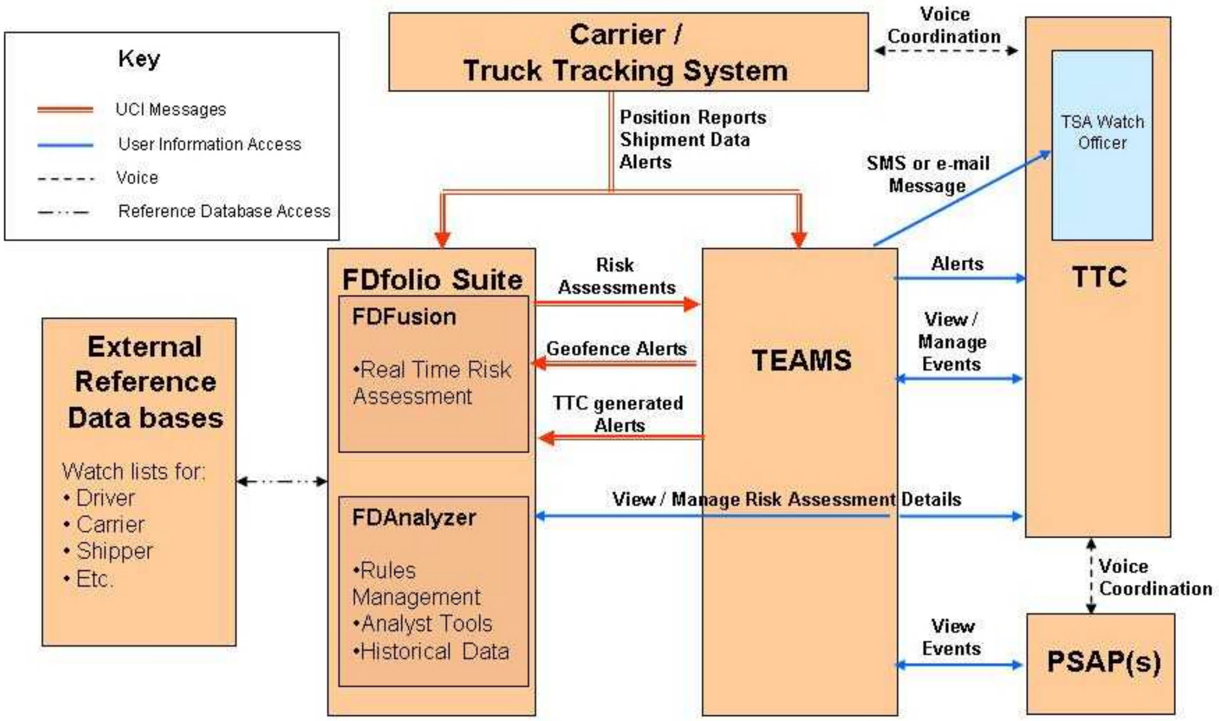
identify high risk situations early enough to initiate a timely response. With this approach, TTC operators are able to analyze and reconcile risks more confidently based on a priority ranking using data that compliments the triggering event information.

In addition to the determination and presentation of risk levels, the TEAMS and FDfolio™ integration supports TTC operators and Watch Officers in resolving high risk situations. Information concerning potential impact areas (e.g., population levels, nearby infrastructure ents), critical contact information (e.g., phone numbers for carrier and local public safety answering point (PSAP)), and a secure mechanism for allowing PSAPs and carriers to access the TEAMS displays.

TSA is also able to access FDfolio™ via a link from TEAMS. Once within FDfolio™, TSA staff may then disable rules based on information from the carrier or truck tracking center. TTC Operators Watch Officers, and / or Managers are able to use TEAMS to create a Transportation Security Incident (TSI) when determined to be appropriate.

Figure 1.23 provides an overview of the risk assessment architecture. It shows key systems, data sources, and the interfaces to the TTC and PSAPs.

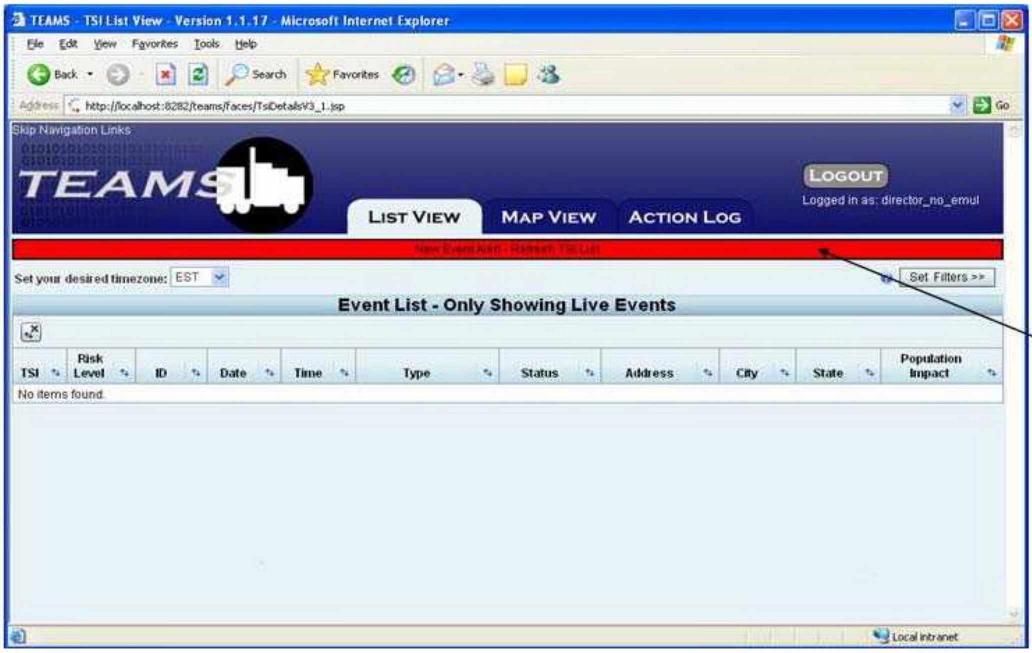
Figure 1.23 The HTSP risk assessment architecture



1.11.2 TEAMS was modified to help truck tracking center operators monitor shipments with high risk scores.

The following sequence of TEAMS screen shots in **Figure 1.24** illustrates what a TTC operator sees when a hazmat shipment is a security risk.

Figure 1.24 TEAMS screenshots – security risks



TEAMS - TSI List View - Version 1.1.17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8282/teams/faces/TsiDetailsV3_1.jsp
Go
Skip Navigation Links
TEAMS
LOGOUT
List View
Map View
Action Log
Set Filters >>
Local intranet

Logged in as: director_no_emul

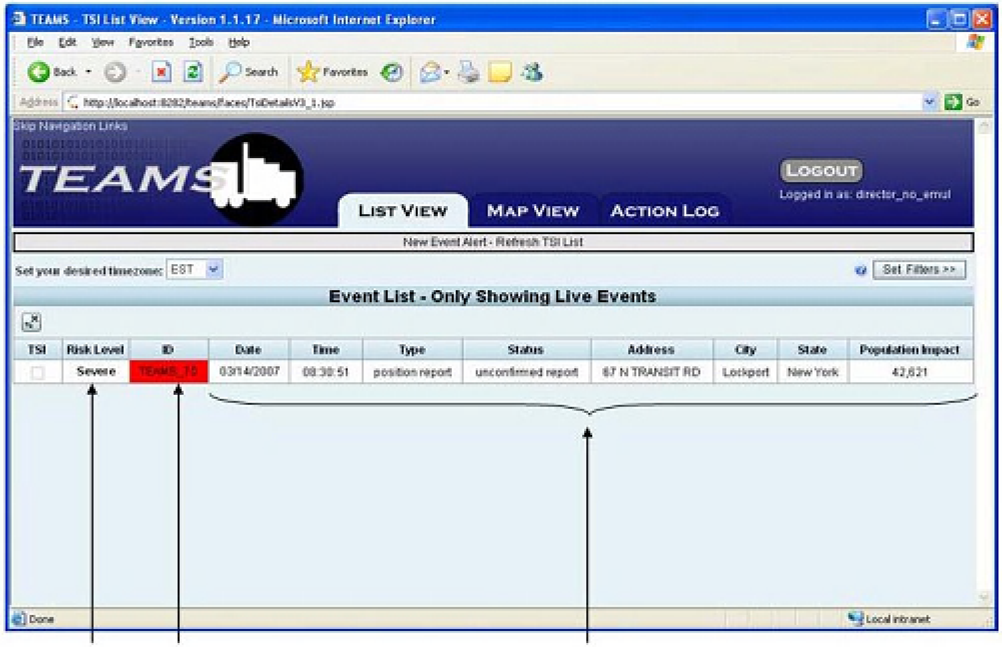
New Event Alert - Refresh TSI List

Set your desired timezone: EST

Event List - Only Showing Live Events

TSI	Risk Level	ID	Date	Time	Type	Status	Address	City	State	Population Impact
No items found.										

Alert bar indicates high risk situation; click on bar for details



TEAMS - TSI List View - Version 1.1.17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost:8282/teams/faces/TsiDetailsV3_1.jsp
Go
Skip Navigation Links
TEAMS
LOGOUT
List View
Map View
Action Log
Set Filters >>
Done
Local intranet

Logged in as: director_no_emul

New Event Alert - Refresh TSI List

Set your desired timezone: EST

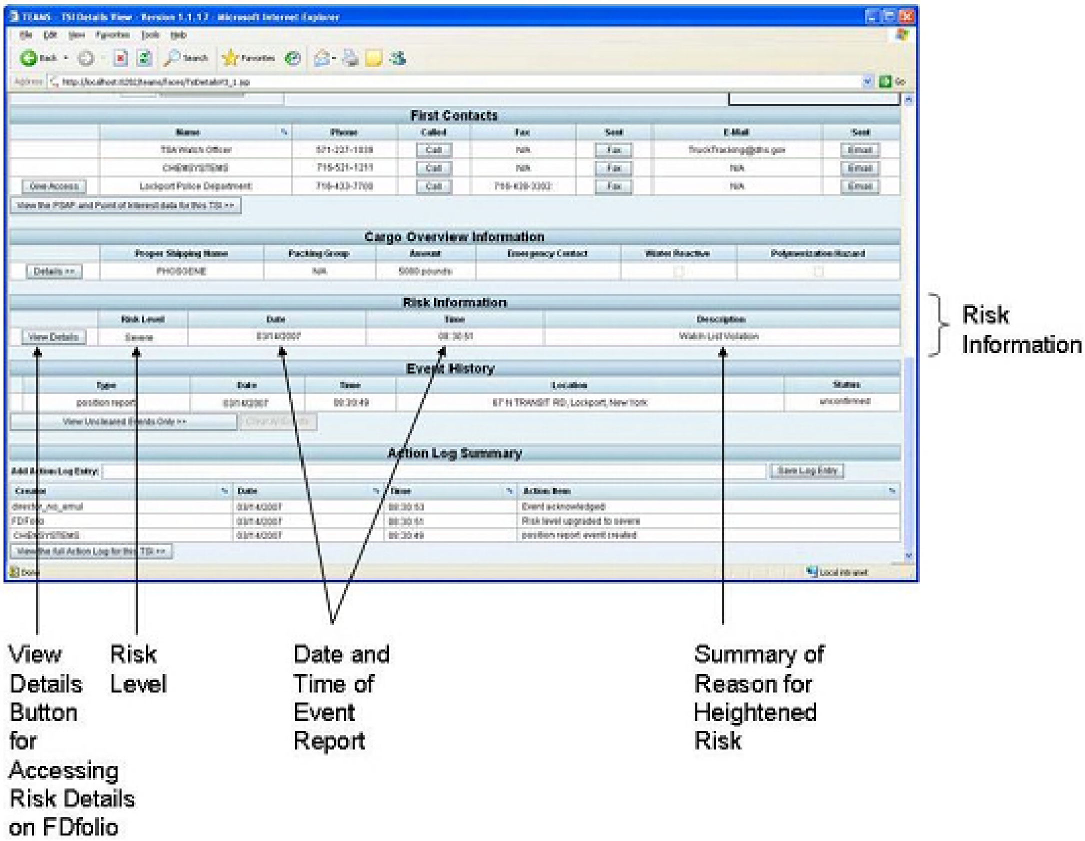
Event List - Only Showing Live Events

TSI	Risk Level	ID	Date	Time	Type	Status	Address	City	State	Population Impact
□	Severe	TEAMS_19	03/14/2007	08:30:51	position report	unconfirmed report	87 N TRANSIT RD	Lockport	New York	42,621

Risk Level

Click on Incident ID For Detailed Information

Event Summary Information



TEAMS - TSI Details View - Version 1.1.17 - Microsoft Internet Explorer

http://localhost:8282/teams/faces/TsiDetail/f3_1.jsp

First Contacts

	Name	Phone	Called	Fax	Sent	E-Mail	Sent
	TSA Watch Officer	571-227-1038	Call	N/A	Fax	TruckTracking@dhs.gov	Email
	CHEMSYSTEMS	716-521-1211	Call	N/A	Fax	N/A	Email
Give Access	Lockport Police Department	716-433-7700	Call	716-439-3302	Fax	N/A	Email

View the PSAP and Point of Interest data for this TSI >>

Cargo Overview Information

	Proper Shipping Name	Packing Group	Amount	Emergency Contact	Water Reactive	Polymerization Hazard
Details >>	PHOSGENE	N/A	5000 pounds		□	□

Risk Information

	Risk Level	Date	Time	Description
View Details	Severe	03/14/2007	08:30:51	Watch List Violation

Event History

Type	Date	Time	Location	Status
position report	03/14/2007	08:30:49	67 N TRANSIT RD, Lockport, New York	unconfirmed

View Uncleared Events Only >> Clear All Events

Action Log Summary

Add Action Log Entry: Save Log Entry

Creator	Date	Time	Action Item
director_no_email	03/14/2007	08:30:53	Event acknowledged
FDFolio	03/14/2007	08:30:51	Risk level upgraded to severe
CHEMSYSTEMS	03/14/2007	08:30:49	position report event created

View the full Action Log for this TSI >>

Risk Information
View Details Button for Accessing Risk Details on FDfolio
Risk Level
Date and Time of Event Report
Summary of Reason for Heightened Risk

1.11.3 Dynamic risk profiling requires a substantial amount of data; much of the needed data was not available during the pilot.

Dynamic risk profiling is important, but the HTSP pilot could only confirm that it is possible to achieve it. Lack of data and development of workable business rules constrained what was possible.

The success and effectiveness of a risk-based solution for hazmat shipment tracking depends on the adequacy of the data that it uses. The data will need to be available in a timely manner and in a usable form. It will also need to be reliable.

Three types of data are needed to support the HTSS risk-based solution: event data, reference data, and watch list data. Each of these is described below.

- Event data. Event data is generated by the shipment itself. It includes data describing the shipment (e.g., shipping organization, consignee, carrier, contents, etc.), data defining events associated with the shipment (e.g., panic button, missed gate-in, etc.) and the updates to the location of the truck.
- Reference data. Reference data is used to associate a shipment with levels of risk. It includes data associated with the material being shipped (e.g., toxicity, explosiveness, etc.), relevant historical information (e.g., past performance of carrier, driver experience, carrier and truck route histories, etc.), and infrastructure information (e.g., location of vulnerable infrastructure).
- Watch list data. Watch list data is maintained by TSA. It identifies carriers, drivers, shippers, and consignees that have high risk profiles (i.e., are known or suspected to be associated with terrorist organizations or have terrorist intentions based on intelligence and / or historical information).

Not all of these data are currently available. As more information is made available the ability to define rules for estimating risk levels will improve. At a minimum, it is necessary to provide basic shipment data (i.e., carrier identification, event type). Shipment contents data is also recommended and can currently be assessed using existing rules in FDfolio™. With this basic data, TEAMS and FDfolio™ can make basic risk assessments. As more data becomes available, more accurate and valid risk assessments will be possible.

Historical data and rules for evaluating shipments against historical norms can be developed over time and managed by FDfolio™. For example, normal routes and movement behaviors by truck and carrier can be collected and stored by the system in confidence, and rules that compare current shipments to these historical data can be developed. With these data and rules, FDfolio™ can compare current shipment information (e.g., updated truck location) to "normal" behavior for that carrier or truck in conjunction with other factors to determine a composite risk level. Over time, more complete historical data can be developed, continually improving the overall risk assessment.

Figure 1.25 summarizes the data categories and indicates the data that was available during the HTSP. This table also presents the data that are required by the risk assessment process as it is currently implemented.

Figure 1.25 Data availability during the HTSP program.

Event Data			
Shipment Data	Planned route	**No**	Not available – no electronic routes from carriers
	Vehicle ID	Yes	
	Origin-destination	**-**	Only one carrier provided origin-destination information
	Shipper	**-**	Only one carrier provided shipper information
	Carriers	Yes	
	Consignee	**-**	Most carriers refused to provide information
	Driver	**No**	No - but simulated in test
	Cargo (material)	**-**	Inconsistent
	Cargo (quantity)	**-**	Inconsistent
Event Type (real time)	Truck sensor data	**No**	
	Shipment off course	**No**	
	Overdue shipment	**No**	
	Geo-fence violation	Yes	Determined by TEAMS
	Missed gate-in	**No**	
Vehicle	Vehicle data (e.g., VIN, year, make, model, registration numbers, plate)	Yes	Database, accessed based on Vehicle ID
Carrier	Company name and ID	Yes	Database, accessed based on Vehicle ID
	Contact name	Yes	Database, accessed based on Vehicle ID

Watch List Data			
Watch List Type	Driver	**No**	
	Carrier	**No**	
	Shipper	**No**	
	Consignee	**No**	
Reference Data			
Material	Class and division (e.g., toxic by inhalation, explosive, etc.)	Yes	Available from Emergency Response Guide (ERG), material data sheets (MDS), etc.
	Isolation zone	Yes	
Shipper, Consignee	Historical profiles - material (e.g., materials, quantities, carriers, consignees, etc.)	**No**	Can be developed by FDfolio™ over time. Not currently included in pilot system.
Carrier	Historical profiles - material (e.g., materials, quantities, carriers, consignees, routes, etc.)	**No**	Can be developed by FDfolio™ over time. Not currently included in pilot system.
	Historical profiles - routes (e.g., planned vs. actual routes, fixed vs. ad hoc, schedules.	**No**	Can be developed by FDfolio™ over time. Not currently included in pilot system.
Driver	Background (e.g., experience, citizenship, demographics, criminal history)	**No**	Can be developed by FDfolio™ over time. Not currently included in pilot system.
Hazmat Industry	Shipments patterns, statistics	**No**	Can be developed by FDfolio™ over time. Not currently included in pilot system.
Critical Infrastructure	Population impact	**No**	Calculated by TEAMS and made available to HTSS users but not communicated to FDfolio™. This was simulated during a walkthrough demonstration.
	Infrastructure impact	**No**	Nearby infrastructure provided by TEAMS and made available to HTSS users but not communicated to FDfolio™.

1.11.4 The rules engine in FDfolio™ was populated with a set of simple rules; future rules will provide deeper risk insight.

The HTSP operational deployment implemented a small set of rules in order to demonstrate and test the risk-based concept. **Figure 1.26** lists rules that were applied during the HTSP program.

Figure 1.26 Future business rules for hazmat shipments

Rule	When Applied	FDfolio™ Action
Shipment-score-baseline-commodity-shipment	Shipment Initiation	FDfolio™ assigns risk score based on commodity Each commodity consequence factor is managed independently. Default commodity score is 100. Score can be changed via the UI.
Shipment-unknown-driver	Shipment Initiation	Checks if the Driver is on the known driver list - gives score of 200 if not.
Position report	Each UCI Event	No risk score change, positional data stored in database
Driver alarm	Each UCI Event	Increments score by 400 if driver alert UCI event is received
Vehicle hijack	Each UCI Event	Increments score by 500 if hijack UCI event is received.
Entered geo-fence	Each UCI Event	Increments score by 50 if exclusionary zone entry UCI event is received.
Exited geo-fence	Each UCI Event	Decrements score by 50 if exclusionary zone is exited UCI is received.

These rules are only an initial sample of those that may eventually be applied. Much greater risk management functionality can be built into a hazmat truck tracking systems with a more extensive set of rules. Future rules will likely fall into one of the following categories.

- **Cargo Analysis.** Rules in this category consider the nature of the cargo being shipped and assess risk inherent in this cargo (i.e., a risk score is assigned for each material, additional rules can be added that are associated with a category of materials)

- **Modal Analysis.** Rules in this category assess risk associated with the shipment mode, perhaps in combination with a particular chemical. For example, in the HAZMAT truck situation compared to rail, a higher risk score could be assigned because trucks can be driven to specific targets or because they are more susceptible to a particular type of attack that may be expected based on available intelligence.

There are many types of business rules that might be developed for hazmat shipments.

- **Entity Analysis**. Rules in this category consider entities associated with a shipment. For example, a particular consignee may be a source of concern based on suspected association with terrorist groups.

- **Event Analysis**. Rules in this category are associated with events. For example, a driver alert or geo-fence violation is assigned pre-specified risk scores. This rule category can look at larger picture issues such as patterns of events across a region or a "swarming scenario" in which multiple shipments are brought together perhaps as part of a coordinated attack.

- **Historical Analysis.** This rule category considers the behavior of shipments compared to historical behavior. For example, when a HAZMAT truck takes an unusual route, follows an unusual schedule, or is carrying an unusual quantity or mix of materials.

- **Consequence Analysis**. Rules in this category consider the potential consequences associated with a particular cargo relative to its current location. For example, a rule can be defined that might define a high risk score because the chemical can be used as a weapon against population centers and the truck is traveling through high population density areas.

1.11.5 Integration of a risk (business rules) engine into a tracking system is feasible and will provide dynamic risk profiling of hazmat shipments.

The HTSP experience proved that it is feasible to connect the standards-based UCI to a risk-based filtering engine such as FDfolio™ to support near real-time risk assessments of hazmat shipments.

The HTSP project team proved that integrating a risk (business) rules engine into a truck tracking system is feasible and will meet TSA's objectives.

During the project, carrier events such as gate-out, position updates, and panic button alerts were forwarded to FDfolio™ by the UCI and successfully processed to evaluate risk level using a small sample of rules. Qualitative risk evaluation scores were returned to TEAMS for display in near real-time. This ability of the UCI to support the required risk-based messaging was demonstrated using the operationally deployed HTSS pilot system.

The risk-based concept, as demonstrated, was analytically shown to reduce false alarms and missed signals over the TEAMS-only approach. This conclusion was reached based on a walkthrough demonstration and a comparative analysis of the ability of TEAMS with and without risk-based support to detect categories of potential threat indicators. The demonstration was based on an actual hazmat shipment that was modified to simulate an evolving security threat situation. Watch list and historical data were simulated to support the scenario.

The analytic comparison of TEAMS with and without risk-based support highlighted several potential advantages of the risk-based approach. These advantages are derived from 1). identification of risk factors not available from a TEAMS-only solution; 2). better ability to consider patterns across multiple shipments; 3). reduced workload with the risk-based approach; and 4). more confident decision-making. More work is needed to develop and validate a more comprehensive rule set before these potential advantages can be realized, however.

The FDfolio™ rules engine was effective in conducting near real-time risk assessments using a small set of rules implemented during the tests. A test version of the HTSS was employed to test FDfolio's™ ability to process input event messages, evaluate risk levels, and support operational tasks associated with the risk-based approach. In addition to verifying the ability of the TEAMS – FDfolio™ integration to provide risk evaluations associated with HAZMAT truck shipment events, these tests evaluated the ability to "drill down" into FDfolio™ to access risk assessment details and rationale. It was possible to accomplish the "drill down" to view specific rule firings and when necessary disable rules "on-the-fly". This capability is intended to support a threat validation process. For example, if non-threatening reasons are found to explain parameters interpreted as threatening the rules involved can be disabled. The tests also verified that risk scores returned to TEAMS from FDfolio™ were consistent with rules that were implemented. It was also possible to integrate new rules into FDfolio™ as experience and evolving threat environments require.

While the feasibility and potential advantages of the risk-based approach were demonstrated, the actual rules implemented were very limited in scope. A more complete set of rules with improved data sources will need to be developed and validated before all the potential advantages can be realized.

These conclusions were specific to the hazmat truck security problem. However, it is notable that a rules-based approach to evaluating risks has been applied to other domains. For example, FDfolio™ has been applied to rail and air hazmat risk assessment domains that involved assessing risks based on hazmat materials and intelligence watch lists.

Valuable risk manager rules were learned in the HTSP program.

1.11.6 Valuable risk management lessons were learned during the HTSP project.

The following risk management lessons from the HTSP project were presented in the final report.

1. **Knowledge of expected behavior is an important consideration.** It is important to have a baseline of expected behavior against which to evaluate hazmat truck actions and assess

associated risk levels. These can be based on normal practice, historical norms for the industry or the specific carrier, pre-planned routes, or regulations (e.g., regulations about travel within high population areas).

2. **Variable update rate for truck location reporting can provide necessary resolution when needed.** As hazmat trucks approach locations that are vulnerable to the particular hazmat being transported it will be necessary to increase the truck location update rate to provide adequate resolution. By increasing the truck location reporting rate only when needed, the costs associated with location reporting can be minimized at other times.

3. **Hazmat-specific risks are an important element of effective risk assessment.** Different hazmat loads are associated with different risks. The risk assessment approach therefore considers the specific hazmat material being transported. For example, high population areas are vulnerable to compressed gases and toxic materials (hazmat material classifications 2 and 6, respectively) while critical infrastructure is vulnerable to explosives, flammable liquids, and flammables (hazmat material classifications 1, 3, and 4, respectively). Behaviors and risks are evaluated based on the hazmat material being transported.

4. **Knowledge of truck contents is essential.** In order to properly assess hazmat risks (as noted above) it is essential that information about what the truck is carrying be made available. The quantity of the material being carried is also important.

5. **Access to watch lists provide a valuable intelligence-based perspective .** Watch lists offer a potentially valuable adjunct to the risk assessment approach because they allow consideration of intelligence information external to the shipment itself. The ability to take advantage of watch lists, however, requires availability of the associated information from carriers (e.g., to use a driver watch list it is necessary to obtain driver information from the carrier).

6. **Things happen fast near targets**. This is a major advantage of the risk-based approach, i.e., that risk-based predictions can provide early warnings. It is important to structure the risk-based approach in a way that provides adequate warning when potential risks occur to allow time for effective actions to be performed. Also, this fact requires that decisions and actions be taken quickly. A key objective of the risk-based approach is to provide early warning, recommendations, and sufficient information about the risks to allow confident and timely decisions. It is equally, important to minimize false alarms to the extent possible to avoid costly and time-consuming responses to non-threats. This is also an objective to the risk-based approach.

1.12 An emulator in the HTSP allowed users to "practice" using the HTSP prototype.

The Emulator page, illustrated in **Figure 1.27**, allows TEAMS users with the appropriate user account privileges to create test events in TEAMS. TEAMS users that do not have Emulator access privileges will not see the Emulator navigation tab when using TEAMS. The Emulator page contains a map that allows a user to enter an event's location, dropdown boxes to set an event's type and status, an area to enter cargo information, and an area to enter vehicle and driver data. Once this data is entered, a user can click a button to create a single test message with the data that had been entered. The Emulator also contains a section that allows a user to create an event that will update automatically by entering a speed, heading, and update rate for the event. The Emulator page also has tabs that a user can click on to navigate to the List View page, Map View page, or Action Log View page.

Truck tracking center operators can practice using the HTSP prototype using the emulator to simulate real events.

The HTSP contractor had to find alternate ways to get cargo data from carriers. One approach involved the use of FDfolio™ to enter cargo data. Another approach was to assign data to "fill in" missing data using a "data publisher."

None of the approaches for capturing cargo data, however, involved the use of an electronic manifest. An electronic manifest would have provided an elegant and functional solution to TSA's needs for hazmat cargo information, especially if the solution integrated with the Customs and Border Protection's ACE Truck E-Manifest.

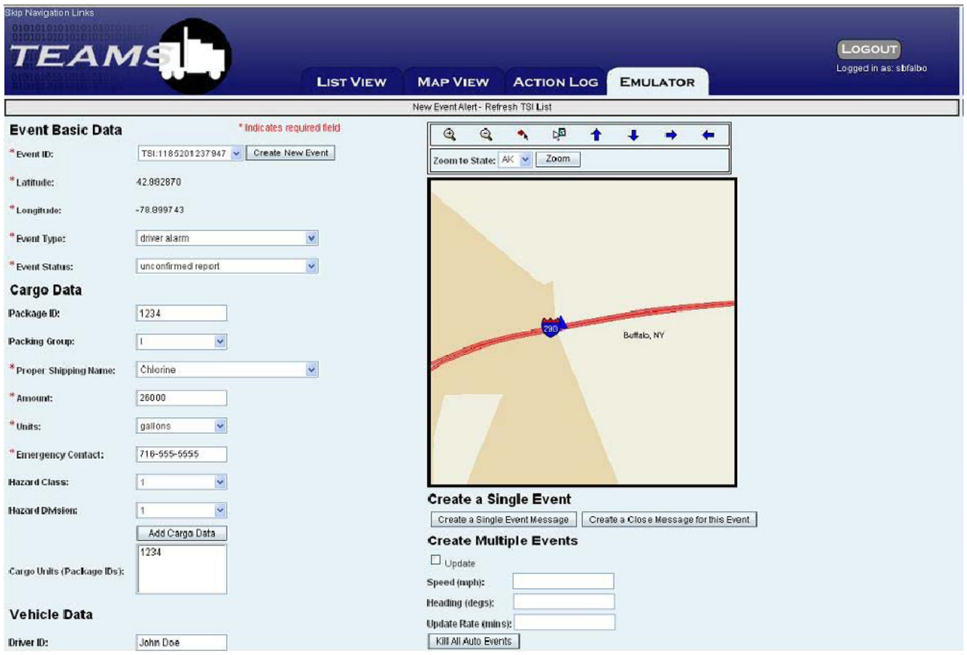
1.13 The HTSP project report suggested enhancements to the prototype.

The HTSP project team suggested numerous enhancements to the prototype.

In its final reports, the HTSP contractor listed a number of enhancements that it expected would be included in an enhanced version of a hazmat truck tracking center.

- Improve the TEAMS user interface by removing the Refresh List button. A graphical component can still be used to flash to get the user's attention in the case of a new alert message being received but new data could be loaded into the list or the

Figure 1.27 TEAMS emulator page



Event Basic Data * Indicates required field

*Event ID: TSI:1185201237947

*Latitude: 42.892870

*Longitude: -78.899743

*Event Type: driver alarm

*Event Status: unconfirmed report

Cargo Data

Package ID: 1234

Packing Group: I

*Proper Shipping Name: Chlorine

*Amount: 26000

*Units: gallons

*Emergency Contact: 716-555-5555

Hazard Class: 1

Hazard Division: 1

Cargo Units (Package IDs): 1234

Vehicle Data

Driver ID: John Doe

Create a Single Event

Create Multiple Events

□ Update

Speed (mph):

Heading (degs):

Update Rate (mins):

Automatically refresh events on the TEAMS user interface – sort the list based on risk to avoid losing sight of important shipments.

map without user interaction. This approach was not originally taken since the List View is sorted by time and the development team felt that automatically loading the newest event data to the top of the list would cause the rows in the list to continually 'jump' from the bottom to the top making it difficult for a user to focus on a row if new data were being received at a high rate. One way to prevent this is to instead sort the list based on risk level or on the internally generated TEAMS ID. If the data is sorted by risk level, the most serious events will be shown at the top of the list for the user.

Enhance vehicle tracking.

- Increase truck location frequency to at least every 15 minutes.
- Establish 2-way communications with fleet tracking vendors.
- Allow carriers to upload electronic route plans.

- Improve vehicle tracking.
  - Increase minimum vehicle location reporting interval to at least once every fifteen minutes, with the capability to increase the frequency if events dictate.
  - Establish two-way communications with truck tracking systems to enable automated requests for reporting rate adjustments.
  - Enhance geo-fencing capability to allow carrier software systems to upload their origin, destination, and current routes.

Improve population at risk calculation features.

- Enhance population impact calculations by considering individual buildings rather than simply calculating percentages of census tract data and considering time of day.

Build features to allow shippers to store information on future shipments.

- Build the capability to accept information on planned shipments as well as active shipments. Planned shipment information would provide analysts the capability to preemptively make decisions on tracking or possibly canceling shipments.

Redesign TEAMS alerting functionality.

- Update TEAMS alerting logic. Most of TEAMS' alerting functionality was not anticipated originally, and a redesign might help identify ways to make it function better.

Make the UI more user friendly by displaying the hierarchical relationships between groups and users.

- Make the User Management graphical user interface more user-friendly so that it is easier for users to determine the hierarchical relationships between groups and users. One way of accomplishing this would be to replace the tables on the main User Management page with a tree structure instead. The currently logged in user's group would be at the top of the tree with all of the subgroups listed underneath. This type of structure would more accurately represent the hierarchical nature of the user accounts in TEAMS. The graphical user interface can also be further enhanced by improving the processing time required to load the pages.

- Tighten integration between TSA and the first responder community by developing electronic data exchange integration capabilities with Computer Aided Dispatch (CAD) systems. The first responders will receive incident information more quickly than they do now and the TEAMS software can receive more detailed information from the first responders when they arrive at the incident scene. Many communities currently have their own CAD systems and data messages can be exchanged using the same 1512 format message that the UCI accepts.

Integrate TEAMS with Computer Aided Dispatch (CAD) systems to better support first responders using the 1512 XML standards.

- Integrate voice over IP (VoIP) within the TEAMS application to allow users to make voice calls over the internet from the TEAMS software rather than using a traditional land-line telephone. One possible method of integration would be to use the API offered by VoIP provider Skype. This API allows developers to utilize Skype's existing VoIP infrastructure in their own custom applications.

Integrate VOIP into TEAMS to eliminate use of land-lines to communicate with system users.

- Improve material handling information:
  - Update the ERG database when the 2008 version of the ERG is released.
  - The isolation zone information is currently displayed as just a distance measure and not contextually related to the event. The isolation information should be graphically displayed using a map that would allow quick identification of any points of interest that might be impacted by material.
  - The ability to perform plume modeling should be considered in conjunction with the isolation zone information.
  - The material handling guides shown are just those related to the materials associated with a given event. The operator should be provided with a means to look up the information for any material, thus allowing for corrections if the material reported is incorrect or no material is reported

Improve hazmat information that TEAMS relies on and passes onto system users.

- Update the map layers used by TEAMS once a year. Also, new vector map overlays that are required by TSA should be added to the TEAMS GIS as needed. The orthographic map capabilities can also be enhanced natively within the TEAMS GIS. If possible, the Google Maps satellite imagery should be replaced with detailed satellite imagery in the TEAMS ArcIMS map service. Doing so will require detailed imagery tiles to be acquired for all of the United States and additional storage space to accommodate all of this data. There may also be potentially significant software modifications to optimize the performance of loading the detailed satellite imagery. However, in the long run decoupling the TEAMS software from the Google Maps service will be beneficial provided that Google may at any time discontinue third parties from using their Google Maps API.

Replace Google Maps imagery with ArcIMS map service.

- Establish a two way communications interface between the truck tracking software packages and the TEAMS software to enable the automated increase of a truck's reporting rate. As the software works now, the same alert is created whether the inner ring or the outer ring surrounding the event violates a geo-fence's boundary. After adding two way communications between the tracking software and TEAMS, a geo-fence violation by the outer ring will not generate an alert to the TEAMS operator but instead automatically increasing the reporting rate for that truck. Then, if the inner ring penetrates a geo-fence's boundary, a message will be generated to alert the TEAMS operator. This will reduce the number of false alarms that are created when the larger outer ring crosses a geo-fence boundary and TEAMS operators will only have to manage events whose inner rings have caused a geo-fence violation.

Establish a two-way communications interface between TEAMS and fleet tracking vendors to enable increased location reporting rate.

- Allow carrier software systems to upload their current routes to TEAMS to make the route adherence feature more feasible operationally. Although computing route deviations is not a technically demanding task, the TEAMS operators may not be familiar with the routes that specific trucks are required to adhere to and this is where the difficulty lies in truly implementing route adherence. This task is best done at the carrier since the route is often more familiar to the carrier's staff. By providing the functionality to allow the carrier to upload its routes to TEAMS and

Provide carriers the capability to load route information into TEAMS.

assign them to specific shipments, route adherence will become a useful feature of TEAMS.

Provide functionality to allow carriers to build a route using start/end locations.

- Add a feature to the geo-fence creation software that allows a TEAMS user to compute a route by assigning a start location and an end location. This will allow a TEAMS user to create a route without having to draw it using the free-form drawing tools. If the carrier's software does not possess the ability to create and transmit routes to TEAMS, the carrier users can use this.

Enhance the population impact feature of TEAMS by basing calculations on house data rather than census tract data.

- Enhance the estimated population impact feature by replacing census tract data with house data. Houses will either be within the isolation zone of an event or outside of the radius and there will no longer be the need to perform the percentage of census tract estimate calculation. Further enhancements can include factoring the local time into population impact calculations. Another data source will need to be provided to TEAMS that will indicate population data in a particular location at various times throughout the day. This data set can provide more accurate results since some areas (like urban business districts) grow in population during the day and shrink in population at night. Advanced plume model analysis can also be used to deliver even more accurate population impact estimates. This would include factoring in weather data to the calculation to determine weather, wind speed, and wind direction which will affect how a chemical spreads when released into the environment. In its current implementation the population impact calculation assumes that the chemical will spread in a perfect circle around the truck.

Provide a messaging capability for carriers via the UCI. Provide user access to TEAMS so that carriers can monitor their fleets.

- Enhance the emulator to provide a full featured data entry page for use by certain TEAMS users. A full featured data entry page will provide the ability to generate live messages that will be sent to the UCI rather than only the test messages sent by the emulator. This enhancement will be useful to participating hazmat carriers that can not automatically generate gate out and gate in messages to send to the UCI. These carriers will be able to login to the TEAMS data entry page and enter information about their trucks and when they are scheduled to depart for their shipments. When the scheduled shipment time elapses, a gate out message can be sent to the UCI and an event will be created in the TEAMS system. Subsequent updates to this event will occur when tracking data is correlated with the event using the truck information. These carriers that use TEAMS for manual data entry will also have access to TEAMS so that they can monitor and track their fleet through the TEAMS software.

Enhance training functionality.

- Enhance in-house truck tracking center training capability.
  - Build a separate system for controlled training to avoid burdening the live and test systems.
  - Build a VoiceXML application to replicate TSA and PSAP responses in a training exercise.
  - Build an analysis tool to evaluate operator performance in handling the simulated events. By analyzing the time statistics for each operator's reaction to the simulated events, it can determine who needs additional training and more efficiently allocate our available training resources.

Add internal system messaging as a safety net to ensure that external alerts receive proper response.

- Provide an external alert (email message, SMS message, etc.) to TSA when an event is not acknowledged by the truck tracking center after a certain time threshold. For example, if an event remains unacknowledged for more than one minute, an email can be sent to TSA brining their attention to this event. This will add an extra layer of notification to help ensure that an actual transportation event does not go undetected by TSA.

Build functionality to improve cargo data input. Replace FDfolio as the mechanism for data input.

- Build a better cargo data interface.
  - Build a cargo data entry application that is explicitly designed for the purpose of tracking hazardous materials. Provide interface information to shippers and carriers so that they may use their existing systems to submit cargo data to the truck tracking center.
  - Discourage the use of FDfolio or similar applications for entering gate-out and gate-in events. The reason for this is that using such an application requires an

operator at the carrier facility to reliably enter the events. A far better solution is using the tracking vendor systems to have the driver create the events.

- Increase the performance and message rate of the HTSP prototype.
  - Increase the speed of PSAP contact information retrieval.
  - Use ArcSDE instead of ArcIMS for PSAP contact queries. ArcSDE is a Spatial Database Engine that allows shapefiles to be stored in a relational database and queried against and is designed to perform high performance geospatial queries.
  - Display PSAP Details Page Data on a map. Adding a map to this page showing the PSAP boundaries in addition to the textual descriptions of the PSAP contact information will be a more complete solution for a TEAMS user. Also, providing the functionality to allow a TEAMS user to make notes about a particular PSAP may be a useful feature. For example, a TEAMS user can make notes about whether or not the PSAP has internet access allowing access to TEAMS or who they spoke with regarding an event. This data could then be retrieved by any user during future communications with this PSAP.
  - TEAMS should be optimized to improve message throughput and user interface performance. To improve throughput, the database storage and geospatial data lookup processes can both be optimized. Performance tuning the Oracle database will increase the speed in which data is written to the database. By implementing a Spatial Database Engine (SDE) rather than performing data queries on a map feature layer service will increase the speed in which geospatial data is queried.
  - Improve user interface processing speed by replacing many of the JavaServer Faces components with more basic HTML components.
  - Improve performance by using partial page refreshes using the Asynchronous JavaScript and XML (AJAX) web programming technique. Instead of requiring an entire page refresh when new data is requested, AJAX will allow a partial refresh of only the data that needs updating considerably improving load time from the user's perspective. For instance, when zooming in on the map, only the map portion of the page should be refreshed, not the entire page. Some of these concepts are applied throughout the geo-fence designer pages and can be applied throughout the entire TEAMS application.
  - Tune Java Virtual Machine (JVM) Heap allocations. The fact that the average CPU load was observed to increase and decrease significantly under a constant message rate indicates that other processes were occupying the CPU time in a less than optimal way. A likely process is memory allocation and garbage collection within the JVM. The JVM heap sizes can be tuned to reduce these peak loads on the CPU and allow for more processing resources for the application.
  - Tune the Thread Pools and Connection Pools. Similar to the JVM heap, thread pools and connection pools can be optimized for the application.
  - Tune the Oracle database. Access by the application to the database is through the Hibernate persistence and query service. This makes measuring the time required for this access difficult to measure at the application level. However tuning the Oracle database to the loads may increase performance.
  - Increase number of processors. After the steps outlined above are addressed, more processor will need to be added to increase the number of truck that can be tracked by the TTCP. The first step may be to run the TEAMS Map server (ArcIMS) on separate dedicated server. Currently it shares a server which hosts the web pages. Also the TEAMS web service and the Oracle database could be hosted on separate servers. Beyond that, clustering of the JBoss Application servers and the Oracle database need to be evaluated.

Increase performance and messaging capabilities of the technology prototype.

- Use ArcSDE to reduce the computational time needed to retrieve geographic information relative to an incident's current location. Currently the ArcIMS product is used to retrieve this information. Although ArcIMS provides this feature, the main role of ArcIMS is to render map images for display on a user interface not to do geo-processing. The optimal product to use for geospatial information retrieval

Use ESRI ArcSDE for geo-spatial data processing/display.

is ArcSDE. The main function of ArcSDE is to do geo-processing tasks such as reverse geo-coding and points of interest lookup. Using ArcSDE instead of ArcIMS to accomplish these tasks will greatly improve the overall performance of TEAMS, especially in a large scale deployment environment where multiple data messages are arriving each second.

- Provide TEAMS users with a more efficient way to manage multiple events.

Enhance TEAMS so that users can manage multiple events – Option 1: multiple windows in the web browser.

  - Option one is to provide a user interface that allows multiple 'windows' to be open within one web browser window that will be more like a 'desktop' that a web page. This option will provide the TEAMS user with a list of all of the events just as the current version does. However, when viewing an event's details the user will not be required to navigate to a new page. Instead of navigating to a separate page, the list will remain visible to the user and a new 'window' will be shown that displays the selected event's detailed information. Multiple 'windows' can be opened at once and each can be dragged, resized, minimized, or closed. This will allow the user to view multiple events at any one time but the interface may become cluttered and confusing if many event details 'windows' are open at once.

Enhance TEAMS so that users can manage multiple events – Option 2: expanded List View.

  - Option two is to provide an expanded List View that displays additional data. This option will be a much less radical change than the previous option utilizing a 'desktop' and 'windows'. In this option, the List View will essentially look the same in its initial state but there will be an arrow icon at the beginning of each row. The TEAMS user may click on this icon to show more data for the selected event without navigating to the full Event Details page. When the arrow is clicked, the row in the table will expand downward and more data will be revealed to the user. This data will include a map of the event's location (either using Google Maps or the TEAMS native ArcIMS service), the first contact information, and Emergency Response Guide data, as well as other data that is identified as this idea is developed. A similar functionality can be added to the Map View page that will allow for the dynamic loading of event details in a portion of the Map View page rather than navigating to the Event Details page. All of these user interface updates and the associated data retrieval will be developed using AJAX techniques so that no page refreshes will occur and the data loading will appear fluid to the user.

Enhance TEAMS so that users can manage multiple events – Option 3: dashboard start page.

  - Option three is to create a 'dashboard' start page with capabilities expanding upon the original List View page. The overview data would still be shown in a list format but an overview map will also be visible on the 'dashboard' page. This will provide an integrated view for the user showing both the list and the map simultaneously. The list will also have the data expansion feature as described above but the map portion will not be displayed in each row. Instead, when the TEAMS user expands the list data for the event, that event's icon will be highlighted on the overview map. This will allow the TEAMS user to see how any of the selected events geographically relate to each other on a single map. The 'dashboard' will initially show the user events with risk scores higher than low risk but filter options will be available natively on the 'dashboard' allowing the user to modify the view as desired without requiring an entire page refresh.

- Modify the TEAMS management approach to improve the ability of TEAMS to handle multiple events simultaneously.

Enhance management capabilities of TEAMS to support multiple events.

  - Filter out position reports and normal shipments by default so that the TEAMS operators are not overwhelmed with information.
  - Add the ability for a TEAMS "manager" to assign resolution of a specific incident to a specific operator on duty.
  - Provide the TEAMS "manager" with a high level overview of all incidents currently in progress to monitor the status of their resolution by the operators.
  - Provide the feature allowing a TEAMS operator can take control of an incident if it hasn't been assigned to another operator yet. This will help reduce any potential bottlenecks of requiring a "manager" to be in the loop of any incident resolution.

- Provide a TEAMS feature that will group incidents that are occurring within the same geographic region. One TEAMS operator can then coordinate with one PSAP call taker about multiple incidents.

blank page

2.0 Independent Verification & Validation Review of the HTSP Technology Prototype [1]

The U.S. Transportation Security Administration employed an independent verification and validation (IV&V) contractor to evaluate the HTSP technology prototype.

The goal of the IV&V effort was to assess if the HTSP technology prototype satisfied program requirements, whether system performance and technical benchmarks were met, and if additional requirements needed to be met in an operational truck tracking system.

The IV&V process implemented on this project by the Evaluation Team was based on industry accepted IV&V approaches to analyze and evaluate software and IT applications and operational testing programs. For the HTSP Prototype system, the Evaluation Team conducted two types of IV&V testing: (1) technical system verification and validation, and (2) evaluation of operations of the HTSP Prototype system. The Evaluation Team also evaluated stakeholder/user issues with the HTSP.

The U.S. Transportation Security Administration employed an independent verification and validation contractor to evaluate the HTSP technology prototype.

2.1 The IV&V contractor identified HTSP technology prototype system defects.

In the area of technical system verification, the Evaluation Team identified 23 system defects. **Figure 2.1** summarizes all the identified defects based on the five defined categories and their associated severity levels, based on High, Medium, or Low levels.

Figure 2.1. Summary of Technical IV&V Testing Results

Severity Level	Functionality	User Interface	System Performance	System Security	Regression	Total
High	1	0	2	2	0	5
Medium	3	1	0	1	0	5
Low	5	6	0	1	1	13
Total **(Percentage)**	**9** **(39%)**	**7** **(30%)**	**2** **(9%)**	**4** **(17%)**	**1** **(4%)**	**23** **(100%)**

Following are brief descriptions of the most serious of these identified system defects:

- **Functional Defects:** Based on the testing results, the geo-fencing functionality is not reliable. For example, events that are supposed to trigger geo-fence violations did not trigger alerts. Events that are linked to a "cleared, removed" geo-fences still incorrectly appear as "entered geo-fence."

- **System Performance:** Two factors significantly slowed down system performance— slow TEAMS response time and the inadequate speed of the map refresh function.

- **System Security:** Unlike typical, password-protected web-based systems, the HTSP system does not time out after a certain amount of idle time. Additionally, web-based systems do not typically store user identification (ID) and password information on the local machine.

The IV&V contractor identified three types of defects in the HTSP technology prototype:

- Functional defects
- System performance defects
- System security defects

[1] This section is taken from the Executive Summary (May 27, 2008) Hazmat Truck Security Pilot (HTSP); U.S. Transportation Security Administration, Transportation Sector Network Management, Highway and Motor Carrier Programs Office; pages 12-23. The Executive Summary was published by TSA as part of its Grant Guidance and Application Kit for TSA FY2009 Trucking Security Program. http://www.tsa.gov/what_we_do/grants/programs/tsp/2009/guidance_application.shtm

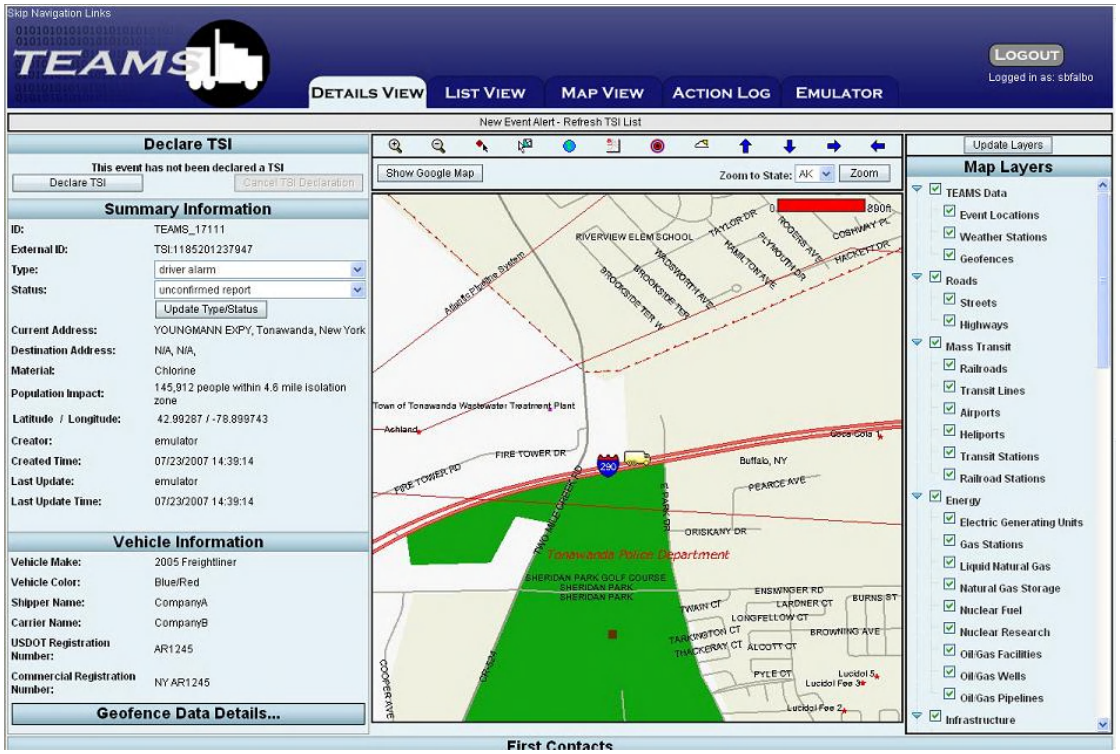
Despite the above system and operations issues, the HTSP Prototype effort demonstrated that the concept for HTSP was feasible and realistic. The testing further highlighted the successful implementation of the non-proprietary Universal Communications Interface set of protocols that will allow alerts and tracking information to be transmitted from all commercially available tracking systems to a prototype truck tracking center (TTC) and a 24-hour Government intelligence operations center.

HTSP staged events were used to identify operational defects in the HTSP technology prototype.

2.2 The IV&V contractor conducted staged events testing to identify HTSP operational issues.

The evaluation team conducted 92 staged events during operational testing. Eight motor carriers, with 124 power units, and 4 different tracking vendors participated in the operational testing. The Evaluation Team conducted the tests between September and December 2007. Operational testing consisted of 46 panic alert events and 46 geo-fence violations, either exclusionary or inclusionary. **Figure 2.2** below shows a TEAMS view of a panic button alert test conducted by the Evaluation Team.

Figure 2.2. TEAMS Details View Page Showing a Driver Alarm.



Declare TSI

This event has not been declared a TSI

Declare TSI | Cancel TSI Declaration

Summary Information

ID:	TEAMS_17111
External ID:	TSI:1185201237947
Type:	driver alarm
Status:	unconfirmed report
	Update Type/Status
Current Address:	YOUNGMANN EXPY, Tonawanda, New York
Destination Address:	N/A, N/A,
Material:	Chlorine
Population Impact:	145,912 people within 4.6 mile isolation zone
Latitude / Longitude:	42.99287 / -78.899743
Creator:	emulator
Created Time:	07/23/2007 14:39:14
Last Update:	emulator
Last Update Time:	07/23/2007 14:39:14

Vehicle Information

Vehicle Make:	2005 Freightliner
Vehicle Color:	Blue/Red
Shipper Name:	CompanyA
Carrier Name:	CompanyB
USDOT Registration Number:	AR1245
Commercial Registration Number:	NY AR1245

Geofence Data Details...

Update Layers

Map Layers

- ☑ TEAMS Data
  - ☑ Event Locations
  - ☑ Weather Stations
  - ☑ Geofences
- ☑ Roads
  - ☑ Streets
  - ☑ Highways
- ☑ Mass Transit
  - ☑ Railroads
  - ☑ Transit Lines
  - ☑ Airports
  - ☑ Heliports
  - ☑ Transit Stations
  - ☑ Railroad Stations
- ☑ Energy
  - ☑ Electric Generating Units
  - ☑ Gas Stations
  - ☑ Liquid Natural Gas
  - ☑ Natural Gas Storage
  - ☑ Nuclear Fuel
  - ☑ Nuclear Research
  - ☑ Oil/Gas Facilities
  - ☑ Oil/Gas Wells
  - ☑ Oil/Gas Pipelines
- ☑ Infrastructure

As part of the testing approach, staged events were established to assess the timeliness and quality of information transfers between the tracked trucks, participating motor carriers, and the Rural Metro operators (acting as the TTC watch standers and representatives from TSA).

Three different staged events were used during the testing: (1) panic alert; (2) exclusionary geo-fence; and (3) inclusionary geo-fence[2]. The events were triggered by drivers in the field or dispatchers located in motor carrier facilities through activation of a panic button, or by violating an established parameter of a geo-fence. For the staged event testing, an exclusionary geo-fence is a defined boundary that a truck must remain

[2] Other attack scenarios can certainly be envisioned beyond those tested, including attempts to mask the GPS signal and then commandeer a truck, attempts to remove HAZMAT cargo from a trailer or tank, or theft of an entire trailer or tank without disruption to the power unit. However, such scenarios were deemed to be outside of the scope of the initial pilot deployment and will be addressed in subsequent tasks of this study.

outside of, whereas an inclusionary geo-fence is one in which the truck must remain within.

The staged event testing process proved problematic, and significant system problems were identified. **Figure 2.3** provides an overview of the types of problems and the level to which they affected the staged event testing.

Figure 2.3. Frequency of Problems/Issues Occurring During Staged Event Testing

Problem/Issue	**Number of Geo-Fence Violation Alerts**	**Number of Panic Alerts**	**Total Combined Alerts**	**Applicable Number of Staged Events**	**Percentage of Staged Events Affected**
The TTC did not receive or respond to alerts.	21	5	26	92	28
TTC was unable to maintain current or multiple carrier contact information.	5	8	13	92	14
TTC watch stander was unable to identify the specific truck generating an alert to the carriers.	20	32	52	92	57
Interpretation of carrier macros to open up a trip, know what the cargo is, and respond to an alert.	19	3	22	92	24
Carriers contacted multiple times for the same event as though a new event had occurred.	1	2	3	92	3
The TTC was overloaded by multiple staged events in short succession.	1	1	2	3	67

The results from the table indicate that two of the problems/issues encountered during the staged event testing occurred in more than 50 percent of the applicable staged events: (1) the TTC was overloaded by multiple staged events in short succession; and (2) the TTC watch stander was unable to identify the specific truck generating an alert to the carriers.

The results also indicate that two of the problems/issues occurred in approximately 25 percent of the applicable staged events: (1) the TTC did not receive or respond to alerts; and 2) interpretation of carrier macros to open up a trip, know what the cargo is, and respond to an alert.

For the portion of the test operations in TEAMS developed by the Evaluation Team that did work successfully in TEAMS, the Evaluation Team focused on measuring the system operational performance of the ***TTC Response Timeline*** to a potential security incident. This timeline is a function of: (1) the time to detect the alert through TEAMS; (2) the time to establish communications with the TSA Watch Officer; and the (3) time to contact the carrier to verify the nature of the alert. Due to the limited data set, this assessment, which included the application of Monte Carlo Simulation, resulted in the following key findings:

- Mean elapsed time of **8 minutes** to complete the *TTC Response Timeline* for panic button alerts.

- Mean elapsed time of **16 minutes** to complete the *TTC Response Timeline* for geo-fence violation alerts.

These findings illustrate that the mean time for both alert types (panic button and geo-fence) was 12 minutes. Based on feedback from the law enforcement community, the time period of up to 12 minutes to confirm an incident and declare a TSI is significantly longer than what would be considered effective for interdiction of a truck, especially in an urban setting. Therefore, a future architecture and Concept of Operations needs to consider that the nearest PSAP or other appropriate incident management lead agency, have access to the alert and receive the same TTC information for alerts at the same time that the TTC receives it. This approach will increase the likelihood that various first responders could respond in a coordinated effort, thereby positioning units to interdict as soon as TSA would declare a TSI.

While the above findings and issues point out to the immaturity of the HTSP system, the testing effort nevertheless demonstrated that a centralized TTC could accept carrier tracking data and respond to panic alerts generated by carriers, as well as alerts resulting from carrier violation of TTC-established geo-fence boundaries.

2.3 The IV&V contractor evaluated stakeholder/user acceptance of the technology prototype.

The Evaluation Team's approach to assessing stakeholder and user acceptance and review of the HTSP system involved active engagement and follow-up with a diverse set of public and private sector groups, including the following:

The IV&V contractor evaluated user acceptance of the HTSP technology prototype.

- **Public Sector:** TSA; Federal Bureau of Investigation (FBI); Nuclear Regulatory Commission (NRC); Department of Defense (DoD); Federal Highway Administration (FHWA); Federal Motor Carrier Safety Administration (FMCSA); Pipeline and Hazardous Materials Safety Administration (PHMSA); Commercial Vehicle Safety Alliance (CVSA); Military District of Washington, D.C.; and Regional/State Law Enforcement (LE) Agencies, Fire Departments, Emergency Management (EM) Agencies, State Transportation Agencies, Hazardous Material/Environmental Agencies, and Academic Institutions.
- **Private Sector:** Motor Carriers; Hazardous Materials Manufacturers and Suppliers; Vehicle Immobilization Technology (VIT) Vendors; Satellite Tracking Vendors; Satellite Communications Providers; Trucking Industry Association; and other private companies.

The Evaluation Team conducted one live and three static demonstrations of the TTC concept to collect information and data from potential HTSP users. The demonstrations took place in Virginia, California, and Washington. The demonstrations used a scripted scenario involving a truck carrying hazardous materials deviating from its assigned route, causing an alert, and prompting the involvement of the TTC, TSA, motor carrier, emergency dispatch, and first responders. The scenario developed into a transportation security incident (TSI), and the TTC facilitated collaboration among the responding agencies and provided access to the HTSP system. The scenario came to a successful conclusion when law enforcement intercepted and stopped the truck.

Immediately following each demonstration session, the audience members participated in focus group or question and answer sessions to assess and document participants' views on the materials and demonstration. Based on the results of these sessions, the Evaluation Team developed a set of focused findings for both the public and private sectors across the following four areas:

ConOps should be changed to provide direct support to first responders in the field.

- **Concept of Operation (ConOps) Issues:** The current ConOps relies on the TTC and its ability to facilitate an appropriate response once an alert is received through TEAMS. Several first responders feel TSA should not attempt to assist in managing emergency response using the TTC capabilities, but rather through the TTC, provide first responders with requested information on the hazmat load and the truck carrying it. The first responders also noted that the concept does not appear to readily allow information and data to be passed from law enforcement personnel in the field to the TTC. A major concern of the first responders is that the concept's protocol, as it is currently designed, results in a process that is too slow, does not involve local responders quickly enough, or provide them the information they need to respond quickly and in a manner safest to the public at large. However, the idea of the TTC notifying jurisdictions and maintaining contact with responders as long as necessary, and in providing all contacted parties with a call-back number in the event more information or assistance is needed also is well received.

- **Other Operational Issues:** One issue raised with the HTSP notification process in that there is no national consistency/standard with the protocol as it is currently designed; there would need to be actual mapping of the emergency response communications network at a national level. There also is concern that the action model does not conform to National Incident Management System (NIMS) or National Response Plan (NRP) (now the National Response Framework as of January 2008); does not use common terminology for incident management; and would not allow for all the needed transportation agencies or organizations at the State and county level to be involved. Some stakeholders also feel that law enforcement at the Federal and State levels should be much more involved in either leading the day-to-day management of the HTSP system or being the first to receive the alert notifications. Additionally, one of the more prevalent operational concerns from the first responders and transportation organizations and agencies involves testing the capacity of the HTSP system to handle multiple alerts and/or incidents simultaneously, and the number of false alarms that the system receives in an alert-rich environment.

The technology prototype does not conform to the National Incident Management System.

- **Regulatory Issues:** One of the most significant issues, and one that warrants further investigation, is how the HTSP program will integrate with other Federal agency programs that regulate hazardous materials. The USDOT, Department of Energy (DOE), Department of Defense (DoD), and the Department of Homeland Security (DHS) are all involved in regulating, in some fashion, the security and safety of hazardous material manufacture, movement, and disposition. Where the HTSP program fits in the scheme of regulatory requirements and how information and data will be exchanged to leverage capabilities is a public sector concern. Also of concern are information sharing and personnel security. Public Law 110-53, ''Implementing Recommendations of the 9/11 Commission Act of 2007,'' more commonly known as the "9/11 Bill," requires TSA to develop a program to track the shipments of certain groups or classes of material in a particular amount or form known as "security-sensitive material" (S-SM). The collaborative process for the HTSP program ConOps involves many "actors" and the concern focuses on how cargo information and data involving S-SM will be protected as it is exchanged.

TSA's truck tracking center should integrate with other federal systems that hold hazmat data and/or provide some type of tracking capability.

For private sector motor carriers the key issue appears to be whether or not participation in the HTSP program will be compulsory or voluntary when it is implemented. Several questions that were raised included that if participation becomes compulsory, what is the anticipated number of motor carriers who will be in the program, the number of loads that will be impacted, what specific data that will be required, and what type of costs were envisioned for the carrier industry associated with participation. Liability is also of concern, as well determining who will be responsible when damage to equipment or injury to personnel occur as a result of or relating to an alert, false alarm, or incident.

Motor carriers who participated in the HTSP Staged Event testing had mixed feelings overall about the usefulness of the HTSP system. Most were very satisfied with their current security equipment and technology used in performing operations; however, not all were as satisfied that the equipment and technology made all of their shipments secure. Regarding the HTSP system process of information dissemination during the staged event testing, most of the motor carriers were satisfied; however, others cited dissatisfaction with presentation of information, usefulness of information, and completeness of information. Regarding the HTSP system procedures for information dissemination during staged event testing, there were varying levels of satisfaction for the motor carriers; however, others cited dissatisfaction with clarity of information from the TTC, completeness of information from the TTC, and consistency of being contacted by the TTC.

2.4 IV&V Conclusions and Recommendations

Figure 2.4 summarizes the conclusions and recommendations of the IV&V contractor. The purpose of the recommendations as stated by the IV&V contractor was to…

"… provide input concerning the future direction of the HTSP program, including the future full deployment of HTSP and TTC technologies in the United States."

Figure 2.4. IV&V Conclusions and Recommendations

Conclusions	Corresponding Recommendations
▪ The HTSP test successfully demonstrated the potential of TTC technologies and standards, including the use of the Universal Communications Interface (UCI).	➢ The high-level TTC concept, which incorporates UCI technologies, should be a cornerstone of the future deployment of the HTSP system.
▪ The HTSP test proved the concept that a centralized TTC could accept carrier tracking data and respond to panic alerts generated by carriers as well as alerts resulting from carrier violation of TTC-established geo-fence boundaries.	➢ While the basic concepts of panic alert information provided to and process by a TTC was validated, additional and significant system re-design will be required to improve the functional reliability of these processes.
▪ The HTSP Prototype system had significant technical performance issues that would need to be addressed before moving to a full-scale system.	➢ In addition to addressing overall system reliability and security issues, the system architecture itself should be significantly revised so that the sluggish system user response issues are corrected; current state-of-the-art technology relating to Web information management software and Web mapping techniques should be leveraged.
▪ The HTSP Prototype system approach to geo-fencing will need significant rework to support a credible TTC operational capability	➢ The current geo-fencing software and operational approach in the HTSP Prototype system should be scrapped. The HTSP Program should investigate the state-of-the-art in geo-fencing applications to identify/ develop a more robust geo-fencing approach for the future deployed HTSP system.
▪ HTSP Staged Event Testing showed a substantial series of system operational problems related to alert notification and TTC communication issues.	➢ The significant HTSP Prototype system errors in alert notification highlights the need for the HTSP program to re-evaluate the current system architecture and ConOps. The errors further underscore the need to establish a formal system engineering and design approach that will ensure the development of a more reliable HTSP system in the near future, as TSA moves forward with deploying a fully operational HTSP system.
▪ Challenges in tracking cargo (trailers/containers) versus power units (truck cabs) remain.	➢ The HTSP program should investigate the current trucking industry deployments of Untethered Trailer Tracking (UTT) systems. These systems would have the advantage of allowing a future HTSP system to track both power units and trailers.
▪ As currently designed, the HTSP Prototype system has significant deficiencies in fulfilling expected first responder requirements.	➢ The HTSP program should establish high-level requirements, possibly through a series of regional "requirements workshops" in each of the Nation's major regions designed to meet congressionally mandated program requirements, while at the same time accommodating the needs and requirements of all stakeholders.

Conclusions	Corresponding Recommendations
■ As currently designed, the HTSP Prototype system does not adequately take into account: (1) how it would integrate with other government security programs and tracking systems; and (2), how it would integrate with established state/local emergency response systems.	➢ Consideration should be given to how this system "fits in" with other systems that are currently in use: (1) determine the impact that the system has on other systems, as well as how it is impacted by other HAZMAT-related Federal regulations and programs; (2) investigate the functional redundancy and uniqueness of TTC operations as related to other tracking programs' operations; and (3), evaluate how the HTSP system could be effectively integrated with other Geographic Information System (GIS)-based emergency response systems.
■ As currently designed, the HTSP Prototype system does not provide the flexibility to accommodate established Law Enforcement/ Emergency Response standards and practices as well as jurisdictional uniqueness.	➢ The following three steps should be considered here: (1) align the system with the NIMS and National Response Framework; (2) ensure the system is adaptable to regional communications protocol, terminology, dispatch procedures, etc.; and (3), establish understandings and agreements with intelligence agencies, fusion centers, and Emergency Operations Centers (EOCs) that help to coordinate correct information transfer.
■ The benefit-cost assessment showed that the system could be deployed by TSA, and initial operations could begin for a budget in the range of $20 million for TSA, which resulted in a significantly positive benefit-cost case for the public sector. However, despite a credible benefit-cost case for motor carriers to deploy the technologies, substantial private sector investment would nevertheless be required to implement the necessary tracking systems.	➢ If a Federal mandate for motor carriers to deploy HTSP technologies is not feasible, then TSA should consider innovative strategies that can leverage the deployment of the HTSP tracking technologies, such as: (1) lower insurance premiums due to reduced levels of risk and improved safety from improved incident detection and response capabilities; and (2) the creation of a deployment incentive tax credit program for the motor carrier industry, vendors, and manufacturers.
■ To support real-time position tracking, the HTSP system may need to receive position reports significantly more frequently (perhaps every 15-30 minutes) than the current industry standard of one report about every 2 hours. The additional cost to TSA and/or TSA of this more frequent position-reporting requirement will be measured in the high tens of million dollars annually.	➢ Additional investigation is required to assess methods of optimizing position reporting based on HAZMAT load type, threat, and consequence information; such optimization has the potential to save TSA and/or industry tens of millions of dollars annually in potentially unneeded communications costs.

blank page

3.0 Gaps Between the HTSP Technology Prototype and a Tier 1 HSSM Truck Tracking System

This section expands on the IV&V analysis of the HTSP technology prototype with a more in-depth look at the gap between the technology prototype and an operational Tier 1 HSSM truck tracking system.

IV&V

The IV&V contractor evaluated the HTSP technology prototype.

It is important to note that the scope of the HTSP project focused on proving that a hazmat truck tracking center was technically feasible and that "smart truck" technology could be crafted into an effective and efficient system for tracking hazmat shipments. It took place before the 9/11 Act directed the TSA Administrator to develop a program to facilitate the tracking of motor carrier shipments of security-sensitive materials. It also was completed before TSA advanced the outlines of a regulatory strategy for Tier 1 Highway Security Sensitive Materials (HSSMs) by issuing voluntary Security Action Items (SAIs) for Tier 1 HSSMs.

The objective of the HTSP project was to prove that a hazmat truck tracking center was technically feasible.

Appendix B describes TSA's Tier 1 HSSM SAIs, and describes the elements of a regulatory program based on Tier 1 HSSM SAI implementation.

As illustrated in **Figure 1.2** on page 3, the HTSP project team began its work in October 2005. It had to make basic assumptions about the regulatory context in which a hazmat truck tracking program might operate, and this factored significantly into design decisions made by the project team. For example, the team could not assume that TSA regulations would drive "smart truck" technology deployment and data reporting, or that hazmat carriers might be obligated to deploy untethered trailer tracking or vehicle immobilization systems.

The HTSP project was completed before TSA issued its Tier 1 HSSM Security Action Item guidance.

Many of the "gaps" between the technology prototype and an operational Tier 1 HSSM truck tracking system are due to TSA programmatic developments that took place after the HTSP pilot program ended.

It's important to stress that the analysis in this section should not be viewed as a negative reflection on the TSA HTSP project or the HTSP technology prototype. The TSA HTSP pilot project conclusively met its objective in demonstrating that "smart truck" technology could be crafted into an effective and efficient system for tracking hazmat shipments. Because of the HTSP program, TSA is now able to state with confidence that implementation of a regulatory program with a hazmat truck tracking system at its heart is completely viable.

The HTSP project was hugely successful in that it proved that a hazmat truck tracking center is feasible from a technology perspective.

It should also be noted that the HTSP project team identified many improvements it believed should be made to the technology prototype (refer to **Section 1.13**, page 33). A number of those recommendations are factored into the analysis under this section. Also, in addition to fully meeting HTSP contract objectives the project team's development of the Universal Communications Interface (UCI) was a particularly notable accomplishment. With only minor modification, the UCI can be incorporated into an operational Tier 1 HSSM truck tracking system.

This section identifies "gaps" between the HTSP technology pilot an operational Tier 1 HSSM truck tracking system.

3.1 The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance.

- TSA Tier 1 HSSM guidance was issued June 2008 – after completion of the TSA HTSP project.
- The technology pilot was not designed with Security Action Item compliance in mind.
- Much of the functionality needed to support a Tier 1 HSSM Security Action Item compliance program is not built into the technology pilot.

- Refer to Appendix B – SAIs of particular note where supporting functionality is lacking or inadequate – SAI#9, SAI#13, SAI#17, SAI#18, SAI#21, SAI#22, SAI#23

3.2 Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype.

IV&V

- Less capable versions of ESRI GIS software was used to build the technology prototype limiting functionality and efficiency of the application.
- Collaboration options in the technology prototype were limited. There was too much reliance on telephone communication in the HTSP concept of operations.

3.3 The technology prototype's alert notification and communications functions were degraded by architectural design flaws.

IV&V

- The IV&V contractor documented significant system errors in alert notification highlighting the need to re-evaluate the current system architecture and concept of operations.
- The errors detected in the technology prototype testing underscored the need to establish a formal system engineering/design approach that will ensure the development of a more reliable operational system.

3.4 The concept of operations underlying the HTSP technology prototype was flawed and substantially incomplete and did not reflect the critical role of states and other parties in securing the hazmat supply chain.

- Only one business process was developed in the HTSP – a driver panic button alert. Many more are needed (see 3.8). The concept of operations plan focused on this alert being distributed to a local public safety answering point (PSAP)[1] for action, bypassing state fusion centers.
- Hazardous materials management is a state-delegated program. In most states, the states – not DOT or TSA – are responsible for the direct regulation and oversight of hazmat carriers. Bypassing state authorities to reach down directly to a PSAP will create a serious state/federal relationship issue. Also, with the development of state fusion centers throughout the nation, states and state fusion centers are a

[1] Wikipedia defines a **Public Safety Answering Point** (**PSAP**) as a call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services. Trained telephone operators are also usually responsible for dispatching these emergency services. Most PSAPs are now capable of caller location for landline calls, and many can handle mobile phone locations as well, where the mobile phone company has a handset location system. Some can also use voice broadcasting, where outgoing voice mail can be sent to many phone numbers at once, in order to alert people to a local emergency such as a chemical spill.

In the United States, the county or a large city usually handles this responsibility. As a division of a U.S. state, counties are generally bound to provide this and other emergency services even within the municipalities, unless the municipality chooses to opt out and have its own system, sometimes along with a neighboring jurisdiction. If a city operates its own PSAP, but not its own particular emergency service (for example, city police but county fire), it may be necessary to relay the call to the PSAP that does handle that type of call. The U.S. requires caller location capability on the part of all phone companies, including mobile ones, but there is no federal law requiring PSAPs to be able to receive such information.

There are roughly 6100 primary and secondary PSAPs in the U.S.. Personnel working for PSAPs can become voting members of the National Emergency Number Association (NENA). Emergency dispatchers working in PSAPs can become certified with the National Academies of Emergency Dispatch (NAED), and a PSAP can become an NAED Accredited Center of Excellence.

better coordination point for initial contact in a transportation security incident. They have more capable systems and communications capabilities than local PSAPs.

- There is a need to drive business processes down to the local PSAP in the event of a transportation security incident (see 3.25 and 3.26), but the business processes for doing so should flow through state fusion centers.

3.5 The HTSP technology prototype relied too heavily on the Universal Communications Interface to bring data into the TEAMS application.

- The IEEE 1512 standards-based Universal Communications Interface (UCI) is an efficient, standards-based mechanism for data intake from fleet tracking vendors.

- Section 1.4 provides an overview of the UCI. **Appendix A** provides links to detailed design documents for the UCI.

- The IEEE 1512 standard was developed to support a wide range of data exchange needs related to hazmat shipments, and hazmat incidents/response. Not all of these data elements were needed to support the HTSP program.

- Hazmat carriers and fleet tracking vendors used the UCI to report data to the technology prototype. Two key pieces of data passed through the UCI – vehicle location and driver panic button alerts. Other data originating from carrier truck-mounted systems will need to flow through the UCI, and the IEEE 1512 standard supports this data flow. This includes alerts from untethered tracking system devices, vehicle immobilization systems, and electronic lock/seals. The incremental cost for additional data reporting from these systems via the UCI is negligible.

- The HTSP technology prototype attempted to use the UCI as the mechanism to capture data on the type and quantity of materials in hazmat shipments. While the UCI could be engineered to support this mechanism, it will be much less efficient and more costly to implement than an electronic manifest (see Section 3.6). Data submission by the UCI will also place a larger burden on Tier 1 HSSM carriers and fleet tracking vendors. Data intake through the UCI should be strictly limited to data naturally flowing from truck-mounted "smart truck" devices.

3.6 The technology prototype did not employ an electronic manifest solution that would allow it to efficiently accept load, driver, & shipment information.

- The original concept of the UCI was that the truck tracking center (TTC) would receive a message containing location, cargo manifest and event data from the fleet tracking vendor. The carrier's gate out message – routed from the fleet tracking vendor to the TTC - would include the cargo manifest information and truck identification information. During the course of the shipment, the truck would provide position updates, and provide updated location data and alerts (as needed). Finally, assuming normal completion of the shipment, the driver would provide a gate-in indication.

- Section 3.5 touched on some of the reasons the UCI is not the most efficient mechanism for bringing cargo manifest data into the truck tracking solution. Beyond type and quantity of the materials in a shipment, Tier 1 HSSM shipping papers (manifests) will include many more data elements. The Custom and Border Protection's ACE truck e-manifest, for example, has 70 data elements including many that would be necessary in a Tier 1 HSSM manifest. Trying to push a large number of data elements through the UCI would not be possible.

- An e-manifest solution based on XFML e-forms technology will be a more efficient and effective mechanism for loading data on shipment transactions into a truck tracking center. Refer to **Appendix C** for an overview of e-forms technology.

3.7 The HTSP technology prototype user interface was built to serve the needs of the security specialist that monitors hazmat shipments, however, other users also need to use the system.

- The technology prototype was built with one graphical user interface (GUI), the GUI for the security specialist that will monitor hazmat shipments. There will be other truck tracking system users beyond the security specialist, however.

- Portals for Tier 1 HSSM shippers and carriers will require new user GUIs. Also, TSA and state fusion center personnel will need GUIs to meet their needs. In addition, internal truck tracking center personnel other than Security Specialists may need GUI's specific to their business requirements (i.e. watch officer, intelligence analyst, etc.).

3.8 Only one business process workflow was served by the technology prototype - many more are needed to support TSA's requirements for a Tier 1 HSSM truck tracking system.

- The HTSP project developed only a single workflow/business process – panic button alert by a hazmat driver.

- Many more business processes/workflows need to be served in a Tier 1 HSSM truck tracking system. A few examples of business processes that would need to be served include the following.
  - Vehicle off route
  - Unanticipated trailer disconnect
  - Large jump in shipment risk score
  - Unauthorized driver attempts to pick up shipment

3.9 The panic button business process workflow/system in the HTSP technology prototype did not work effectively and efficiently.

IV&V

- The IV&V report criticized the speed and reliability of the panic button alert workflow in the HTSP technology prototype.

- According to the IV&V contractor,

> *"While the basic concepts of panic alert information provided to and processed by a TTC was validated, additional and significant system re-design will be required to improve the functional reliability of these processes."*

3.10 Tier 1 HSSM shippers and carriers, important external stakeholders in TSA's hazmat program, have workflow needs that the technology prototype did not meet.

- Tier 1 HSSM shippers and carriers will be important external stakeholders in a Tier 1 HSSM truck tracking system.

- As noted in 3.8, the HTSP technology prototype only developed one workflow. Many more will be needed in a fully operational Tier1 HSSM truck tracking system.

- Tier 1 HSSM shippers and carriers will likely use the Tier 1 HSSM system to perform a number of functions including registration, e-manifest preparation/submittal, e-route preparation/submittal. Workflows associated with these functions will need to be developed.

3.11 The business rules engine effectively applied only one rule. The rules engine was embedded in a "black box" commercial product and rules could not be easily authored or modified.

- A business rules engine is essential to developing a dynamic risk score for hazmat shipments. The technology prototype demonstrated that integrating a business rules engine in a truck tracking system was practical.
- The business rules engine capability in the HTSP technology prototype was supplied by the FDFolio™ product. The business rules engine was, however, part of the "black box" of the commercial FDFolio™ product and could not be configured easily.
- Only one business rule was developed in the technology prototype. In practice, many more will be needed. **Appendix C** discusses the different types of business rules engines and how they might be configured in a truck tracking system.
- A COTS business rules engine should be integrated into the truck tracking center. It will be less costly and more efficient. Also, given that business rules will be in constant flux, an easy-to-edit tool is essential.

3.12 The technology prototype did not deploy an electronic route solution that will enable route adherence monitoring.

- Section 1553 of PL110-53 requires *"motor carriers that have a hazardous material safety permit under part 385 of title 49, Code of Federal Regulations, to maintain, follow, and carry a route plan, in written or electronic format".*
- The technology prototype did not deploy an electronic route solution that will enable route adherence monitoring.
- The HTSP prototype did not include functionality for accepting electronic route plans from shippers or carriers. PL110-53 was enacted while the HTSP was underway, and electronic route plans were not included in the HTSP contractor's mission.
- But, electronic route plans are critical to a truck tracking program. Without an electronic route plan, a truck tracking system cannot track carrier route adherence and geo-fence and risk management capabilities of the system will be substantially degraded.

3.13 The technology prototype did not support chain of custody monitoring of hazmat shipments.

- The technology prototype did not advance functionality that would allow system users to preserve and document chain of custody control of hazmat shipments.
- While chain of custody monitoring was not advanced as a Security Action Item, several SAIs (#17, #18, #20) are consistent with the idea that shipment chain of custody be tracked.

3.14 The technology prototype did not deploy an untethered trailer tracking solution.

- The HTSP prototype did not include functionality for untethered trailer tracking (UTT).
- FMCSA's UTT initiative was on-going when the HTSP project began and the HTSP contractor was not tasked with considering untethered trailer tracking in the pilot.[2]
- SAI #23 recommends that Tier 1 HSSM carriers deploy a truck-based monitoring system that includes untethered trailer tracking (UTT) capabilities.
- The FMCSA has developed functional requirements for UTT systems, and it is clear that the technology is suitable for implementation as part of a hazmat truck tracking system.

3.15 The technology prototype did not deploy a vehicle immobilization solution.

- The HTSP prototype did not include functionality for vehicle immobilization.
- FMCSA's vehicle immobilization initiative was on-going when the HTSP project began and the HTSP contractor was not tasked with considering vehicle immobilization in the pilot.[3]
- SAI #21 recommends Tier 1 HSSM carriers deploy a truck-based monitoring system that includes vehicle activation/immobilization capabilities.
- The FMCSA has developed functional requirements for vehicle immobilization systems, and it is clear that the technology is suitable for implementation as part of a hazmat truck tracking system

3.16 The technology prototype did not deploy an electronic lock/seal solution.

- The HTSP prototype did not include functionality for electronic locks/seals.
- SAI #13 recommends that Tier 1 HSSM carriers deploy lock/seal systems.

[2] FMCSA Commercial Motor Vehicle Safety and Security Systems Technology – Untethered Trailer Tracking Systems http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/untethered-trailer-tracking.htm

[3] Federal Motor Carrier Safety Administration; http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/vehicle-disabling.htm

3.17 The geo-fencing solution in the HTSP was based on flawed assumptions about the creation and use of geo-fences by shippers and carriers.

IV&V

- The IV&V contractor recommended that the geo-fencing software and operational approach in the HTSP Prototype system should be scrapped. An operational system should use state-of-the-art in geo-fencing applications to identify/ develop a more robust geo-fencing approach.
- Section 1.10 describes the geo-fencing approach developed by the HTSP contractor.
- The technology prototype approach assumed that system users such as hazmat carriers might be allowed to establish geo-fences in TEAMS. Establishment of numerous geo-fences in the truck tracking system has the potential for generating an overwhelming number of alerts and false positives for Security Specialists.
- The technology prototype also advanced the idea of generating a geo-fence around a truck and using it as a buffer for detecting when a truck is nearing a critical point. In practice, this is an unworkable solution and will create too many false positive alerts.
- A more workable concept of operations approach would restrict geo-fence creation to state and federal security officials. Also, more frequent location reporting would make geo-fence monitoring more viable.

3.18 The database supporting the technology prototype was not designed to support multiple user types, multiple business process workflows and the rich collaboration environment needed in a Tier 1 HSSM tracking program.

IV&V

- Every workflow in a system will generate and/or consume data. As noted in 3.8, only one business process workflow was served in the HTPS. More workflows will require an expanded database.
- Also, functions such as portals, e-manifests, e-routes, UTT monitoring and vehicle immobilization will require an expanded database.
- The IV&V contractor pointed out that the HTSP technology prototype did not employ state-of-the-art technology for web services and GIS services resulting in sluggish performance and poor system reliability.

3.19 The prototype did not support variable location reporting frequency by hazmat carriers (2-way communication).

IV&V

- The IV&V contractor recommended establishment of a two-way communications interface between fleet tracking systems and TEAMS to enable the automated increase of a truck's reporting rate.
- Two-way communications would allow less frequent location reporting to the truck tracking center. Location reporting can be automatically increased as the "risk profile" of a shipment increases and automatically decreased when the risk profile decreases.
- Two-way communications was also recommended by the HTSP contractor.

3.20 The technology prototype only allows a security specialist to manage a single incident.

- There are about 2 million Tier 1 HSSM shipments per year in the United States. This means that a Tier 1 HSSM truck tracking center systems will constantly monitor about 5000 active shipments.
- A business rules engine (see 3.11) will apply dynamic risk modeling algorithms to identify the riskiest shipments to provide security specialists the capability of monitoring the most serious shipments.
- The technology prototype did not allow security specialists to manage multiple incidents – a likely event. In the technology prototype, the security specialist was equipped with a single screen/GUI desktop. A different setup using windows and multiple monitors would allow the security specialist to manage multiple incidents.

3.21 The technology prototype is vulnerable to false positives which could overwhelm security specialists in an operational setting.

- Too many false positive alerts would quickly overwhelm an operational truck tracking center. Geo-fence and route adherence violations could be particularly problematic.
- The technology prototype did not develop the capability to detect and manage false positives. While not a pressing issue in the pilot, full system loading could cause operational failure.

3.22 The technology prototype drew upon a limited set of data from external sources.

- The technology prototype drew on data from fleet tracking vendor systems via the UCI.
- The technology prototype did not, however, draw data from external databases during the pilot. In practice, a Tier 1 HSSM truck tracking system would actively draw on a number of external data sources.

3.23 The technology prototype did not support collaborative exchange with government agencies during a transportation security incident - especially lacking are collaborative tools to support state fusion centers.

IV&V

- As noted in 3.2, collaboration options in the technology prototype were limited. There was too much reliance on telephone communication in the HTSP concept of operations.
- As noted in 3.4, state fusion center collaboration was not built into the concept of operations for the HTSP technology prototype.
- The IV&V contractor noted that the HTSP Staged Event Testing showed a substantial series of system operational problems related to alert notification and truck tracking center communication issues.

3.24 The prototype's design cannot effectively support the transaction volume expected in an operational system.

IV&V

- The transaction volume in an operational system will be about 2 million shipments per year versus only a handful of shipment transactions in the technology prototype.
- Even with limited transaction loading, the IV&V contractor cited sluggish and inefficient performance by the technology prototype.

3.25 The HTSP technology prototype will not meet the operational needs of first responders.

IV&V

- The IV&V contractor stated that the HTSP Prototype system has significant deficiencies in fulfilling expected first responder requirements.
- Collaboration capabilities in the technology prototype are limited.

3.26 The technology prototype is not National Incident Management System (NIMS) compliant and will not support law enforcement and emergency response needs at the state/local level.

IV&V

- The IV&V contractor cited a lack of conformance with the National Incident Management System guidelines.
- NIMS compliance is important to insure that the system will support law enforcement and emergency response needs.

3.27 The technology prototype lacked intelligence analysis capabilities.

- The technology prototype did not have data mining or business analytics functionality.
- Lacking this capability, the ability to anticipate problems before they occur is extremely limited.

3.28 The technology prototype lacked security features that would be required in a system handling business confidential, security-sensitive data.

- Lightweight security features were built into the HTSP technology prototype. An operational system will need strong security functionality.

blank page

4.0 Tier 1 HSSM Truck Tracking System Recommendations

Section 3 identified “gaps” between the HTSP technology pilot and an operational Tier 1 HSSM truck tracking system. This section provides recommendations for addressing those “gaps”. The following figure lists recommendations and associated “gaps”.

Gaps **(from Section 3)**	**Recommendations**
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) Only one business process workflow was served by the technology prototype - many more are needed to support TSA’s requirements for a Tier 1 HSSM truck tracking system. (3.8) The technology prototype did not deploy: • an electronic route solution that will enable route adherence monitoring. (3.12) • an untethered trailer tracking solution. (3.14) • a vehicle immobilization solution. (3.15) • an electronic lock/seal solution. (3.16) The database supporting the technology prototype was not designed to support multiple user types, multiple business process workflows and the rich collaboration environment needed in a Tier 1 HSSM tracking program. (3.18)	**1. Build the truck tracking system to monitor shipments of TSA-designated Tier 1 Highway Security Sensitive Materials in the context of a Tier 1 HSSSM regulatory program based on TSA’s Security Action Items.** • Design the tracking system to serve as the implementing tool for TSA Tier 1 HSSM regulations (Tier 1 HSSM SAIs). Functionality includes: ○ Vehicle tracking ○ Untethered trailer tracking ○ Vehicle immobilization ○ Electronic route plans ○ Electronic manifests (shipping papers) ○ Route adherence monitoring ○ Driver authentication ○ Electronic locks/monitoring ○ Driver panic button/alerts • Full satisfaction of PL 110-53 requirements. Regulated parties (system users) will include Tier 1 HSSM shippers and carriers and fleet tracking vendors. • North American coverage; expected transaction volume about 2 million Tier 1 HSSM transactions/year.
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) The HTSP technology prototype relied too heavily on the Universal Communications Interface to bring data into the TEAMS application. (3.5)	**2. Incorporate the Universal Communications Interface built during the TSA HTSP into the truck tracking center but refine it to support a different concept of operations plan.** • Dataflow from carriers through the UCI should be restricted to vehicle location, gate out/in messages, and alerts from on-board sensors. • Do not use the UCI as the mechanism to capture load or route information. Use shipper/carrier portals for preparation/submission of electronic manifests (load) and electronic route plans. • Do not use the UCI as the mechanism to capture corporate information for a particular shipment. Use shipper/carrier portals to capture corporate data . Draw corporate data from the registration database to support transaction business processes (e-manifests, e-routes, etc.).

The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The HTSP technology prototype user interface was built to serve the needs of the security specialist that monitors hazmat shipments, however, other users also need to use the system. (3.7) Tier 1 HSSM shippers and carriers, important external stakeholders in TSA's hazmat program, have workflow needs that the technology prototype did not meet. (3.10)	**3. Build portals with rich functionality for Tier 1 HSSM shippers and carriers; provide 24/7 access to corporate and shipment transaction data.** • Build user portals to allow Tier 1 HSSM shippers/carriers 24/7 access to their data and to allow them to efficiently implement business processes associated with the truck tracking center: e-manifest submission, e-route submission. • Build portals to provide shippers and carriers access to shipment transactions: in-progress and completed. • Every shipper and carrier will have their own portal ("my portal"). Portals will allow company administrators to establish corporate user rights. • Build portals to allow shippers and carriers to complete system registration – i.e. load corporate data into the system database.
Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The technology prototype's alert notification and communications functions were degraded by architectural design flaws. (3.3) The technology prototype did not employ an electronic manifest solution that would allow it to efficiently accept load/driver/shipment information. (3.6) The panic button business process workflow/system in the HTSP technology prototype did not work effectively and efficiently. (3.9) The business rules engine effectively applied only one rule. The rules engine was embedded in a "black box" commercial product and rules could not be easily authored or modified. (3.11) The technology prototype did not support collaborative exchange with government agencies during a transportation security incident - especially lacking are collaborative tools to support state fusion centers. (3.23) The prototype's design cannot effectively support the transaction volume expected in an operational system. (3.24)	**4. Replicate data-merge and data-presentation functions of TEAMS in a truck tracking system but build it using more sophisticated toolsets to optimize speed, functionality, and business process workflow.** • Merge information from the electronic manifest, the electronic route plan, vehicle location, and alerts to answer the following questions (see Figure 1.1). • What is the truck carrying? • What is the shipment risk profile? • Who is driving the truck? • What is the truck's location? • Is there a problem? What? • What is the truck's destination? • What route has the truck followed? • Is the truck off-route? • Deploy XFML technology (e-forms) to build an electronic manifest application to capture load information. Access via portal. • Build an electronic route preparation tool to support easy preparation/storage of carrier-defined routes. Access via portal. • E-manifest and e-route tools will draw on corporate data captured though registration. • Use latest GIS and portal (collaboration) tools to support development of the truck tracking center. • Build to efficiently process expected Tier 1 HSSM transaction traffic – 2 million transactions/year.
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) The HTSP technology prototype user interface was built to serve the needs of the security specialist that monitors hazmat shipments, however, other users	**5. Substantially expand the list of workflows/business processes served beyond those currently served by TEAMS.** • The only business process addressed in the HTSP was the process associated with a driver panic button alert.

also need to use the system. (3.7) Only one business process workflow was served by the technology prototype - many more are needed to support TSA’s requirements for a Tier 1 HSSM truck tracking system. (3.8) Tier 1 HSSM shippers and carriers, important external stakeholders in TSA’s hazmat program, have workflow needs that the technology prototype did not meet. (3.10) The technology prototype did not deploy: • an electronic route solution that will enable route adherence monitoring. (3.12) • an untethered trailer tracking solution. (3.14) • a vehicle immobilization solution. (3.15) • an electronic lock/seal solution. (3.16)	The HTSP concept of operations was built around the actions that would be taken in the event of a panic button alert. • To support TSA’s SAIs, the system will need to serve specific business processes associated with the SAIs. For example, what needs to be done if: • An unauthorized driver attempts to pick up a Tier 1 HSSM shipment (SAI #6)? • A trailer is unexpectedly detached from a tractor during a shipment (SAI #23)? • A truck is substantially late or off-route of its expected route (SAIs #17,18)? • An electronic lock is breached during transit (SAI #13)? • Workflows need to extend beyond the Security Specialist desktop to TSA. State fusion centers, emergency responders, etc.
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The technology prototype did not deploy an electronic route solution that will enable route adherence monitoring. (3.12)	**6. Incorporate an on-line electronic route plan tool into the system for shippers/carriers to use to prepare and submit e-route plans via a portal.** • Build an electronic route authoring tool accessible to shippers and carriers via their portals. Use advanced GIS tools to build the e-route authoring tool. • Shippers/carriers can create and store e-routes on-line. They can retrieve them when needed and associate the e-route with a shipment as needed. • Electronic route plans must be submitted at or before “gate-out”. The route followed by a carrier from “gate-out” to “gate-in” will be stored on shipper/carrier portals.
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The HTSP technology prototype relied too heavily on the Universal Communications Interface to bring data into the TEAMS application. (3.5) The technology prototype did not employ an electronic manifest solution that would allow it to efficiently accept load/driver/shipment information. (3.6) The technology prototype did not support chain of custody monitoring of hazmat shipments. (3.13)	**7. Incorporate an XFML-based electronic manifest tool into the system for shippers/carriers to use to prepare and submit e-manifests via a portal**. • Build an electronic manifest authoring tool accessible to shippers and carriers via their portals. Use an xfml e-forms tool to build the electronic manifest tool. • Shippers/carriers can create and store electronic manifests on-line. They can retrieve them when needed to support a shipment. • Electronic manifests must be submitted at or before “gate-out”. Electronic manifests from completed transactions will be stored on shipper/carrier portals.

Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The geo-fencing solution in the HTSP was based on flawed assumptions about the creation and use of geo-fences by shippers and carriers. (3.17) The prototype did not support variable location reporting frequency by hazmat carriers (2-way communication). (3.19)	**8. Scrap the geo-fencing approach used in the TSA HTSP; rebuild using upgraded GIS tools.** • Build a geo-fencing authoring tool using advanced GIS tools. • Only authorized state and federal users will be allowed to create a geo-fence in the system. • Geo-fences can have a wide range of attributes. A modeling tool will support analysis of the impact of each geo-fence on workload before the geo-fence may be loaded into the system. • Geo-fences must be "reauthorized" periodically to avoid being purged from the tracking system.
The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1) The technology prototype did not deploy: • an untethered trailer tracking solution. (3.14) • a vehicle immobilization solution. (3.15)	**9. Build the truck tracking center system to support untethered trailer tracking and vehicle immobilization.** • The UCI will be the path for alerts. • Business rules risk scoring will likely push scores up high enough to require immediate attention of Security Specialists. • Workflows specifically built for each scenario will support investigation/resolution by the Security Specialist.
The HTSP technology prototype user interface was built to serve the needs of the security specialist that monitors hazmat shipments, however, other users also need to use the system. (3.7) The technology prototype lacked intelligence analysis capabilities. (3.27)	**10. Build desktops to meet the operational needs of personnel serving in the truck tracking center including security specialists and intelligence analysts.** • Security specialists will monitor shipments 24/7 and respond to issues arising with in-transit shipments. • Intelligence analysts will react to security alerts from TSA and modify business rules to reflect immediate issues. Analysts will also identify issues and anomalies in shipments to prevent or mitigate incidents. • Other desktops might include a watch commander desktop and a user support desktop.
Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The technology prototype's alert notification and communications functions were degraded by architectural design flaws. (3.3) The database supporting the technology prototype was not designed to support multiple user types, multiple business process workflows and the rich collaboration environment needed in a Tier 1 HSSM tracking program. (3.18)	**11. Rebuild the security specialist's desktop application to support management of multiple incidents and to serve collaboration needs with TSA, state fusion centers, hazmat carriers/drivers, and first responders.** • Security specialists will likely use multi-screen workstations, and will need to be able to manage multiple incidents/issues at a time. • Security specialists need to call upon a mix of communication tools to meet workflow needs. For example, if the workflow calls for a conference call with TSA and a state fusion center, the Security Specialist

The technology prototype only allows a security specialist to manage a single incident. (3.20) The technology prototype did not support collaborative exchange with government agencies during a transportation security incident - especially lacking are collaborative tools to support state fusion centers. (3.23)	should be able to initiate the call automatically from the desktop. • Security Specialists should be able to collaborate efficiently with state fusion centers and first responders. Collaboration tools need to support efficient workflow from the truck tracking center all the way down to the field level.
Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The business rules engine effectively applied only one rule. The rules engine was embedded in a "black box" commercial product and rules could not be easily authored or modified. (3.11)	**12. Build a stand-alone business rules engine into the truck tracking center using a COTS software product.** • Use a powerful COTS business rules engine as a stand-alone tool – i.e. not integrated into a "black box" application. • The business rules engine should be easy to modify "on the fly" by business analysts. • Rule processing – especially alert processing - must be almost instantaneous.
The business rules engine effectively applied only one rule. The rules engine was embedded in a "black box" commercial product and rules could not be easily authored or modified. (3.11) The technology prototype only allows a security specialist to manage a single incident. (3.20) The technology prototype is vulnerable to false positive which would overwhelm security specialists in an operational setting. (3.21)	**13. Use the business rules engine to support dynamic risk profiling and to manage work load at the truck tracking center.** • The business rules engine will create a risk score for a shipment at "gate-out". Risk scoring will be updated continuously between "gate-out" and "gate-in". For example, every location update will result in rescoring for a shipment. • While the application will likely start with a simple set of rules, the rules may grow in complexity over time to reflect TSA's risk outlook. • Rules should always be tested before live loading to avoid overwhelming the truck tracking center with low priority alerts.
The geo-fencing solution in the HTSP was based on flawed assumptions about the creation and use of geo-fences by shippers and carriers. (3.17) The prototype did not support variable location reporting frequency by hazmat carriers (2-way communication). (3.19)	**14. Build 2-way communications capabilities between the truck tracking system and fleet tracking vendor systems to manage data reporting (variable reporting frequencies).** • SAI #23 recommends location reporting every 15 minutes. Depending on the risk profile of the load, a 15 minute reporting interval may be over-reporting or under-reporting. • Fleet tracking vendors' systems must be able to accept an automated request from the truck tracking center to adjust reporting frequency. • For low-risk shipments in sparsely populated areas, reporting intervals >> 15 minutes may be sufficient. For high-risk shipments in sensitive areas, reporting intervals < 15 minutes may be needed.

Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The concept of operations underlying the HTSP technology prototype was flawed and substantially incomplete and did not reflect the critical role of states and other parties in securing the hazmat supply chain. (3.4) The technology prototype did not support collaborative exchange with government agencies during a transportation security incident - especially lacking are collaborative tools to support state fusion centers. (3.23)	**15. Build an interface between the truck tracking center and state fusion centers to enable coordinated response to transportation security incidents.** • State fusion centers are a key point of contact for the truck tracking center, and many business processes will involve communication/collaboration with fusion center staff. • Collaboration must be efficient, fast, and easy. Automated or desk-top initiated communication will be a key feature of the Security Specialist desktop. • Collaboration must flow through the state fusion center down to first responders in the field. • A state fusion center will have access to its state's "common operating picture" (COP). The state's COP will include data on shipments originating or ending in the state as well as shipments passing though the state. The COP will feature a map visualization of in-transit shipments. • In the event of a transportation security incident, truck tracking systems will automatically initiate contact with the state fusion center and "push" information on the shipment to the fusion center. • The truck tracking center will have a "response toolkit" available to support the state and first responders in the event of a declared security incident, and will provide support and assistance until the incident is resolved.
Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2) The concept of operations underlying the HTSP technology prototype was flawed and substantially incomplete and did not reflect the critical role of states and other parties in securing the hazmat supply chain. (3.4) The technology prototype did not support collaborative exchange with government agencies during a transportation security incident - especially lacking are collaborative tools to support state fusion centers. (3.23) The HTSP technology prototype will not meet the operational needs of first responders. (3.25) The technology prototype is not National Incident Management System (NIMS) compliant and will not support law enforcement and emergency response needs at the state/local level. (3.26)	**16. Build a NIMS-compliant communications infrastructure that will support efficient collaboration during a transportation security incident.** • Truck tracking center systems and business processes will be NIMS-compliant. • Extend business processes/workflows though the state fusion centers to emergency responders. • As noted in #15, the truck tracking center will support state fusion centers, local governments, and first responders in the event of a transportation security incident. • As noted in #4, state-of-the-art communications and collaboration tools will be used to support the interface between the truck tracking center and state fusion centers.
The technology prototype drew upon a limited set of data from external sources. (3.22) The technology prototype lacked intelligence analysis capabilities. (3.27)	**17. Build intelligence analysis capability into the truck tracking center.** • Build an intelligence analyst desktop to support the capability to anticipate and prevent security incidents.

The concept of operations underlying the HTSP technology prototype was flawed and substantially incomplete and did not reflect the critical role of states and other parties in securing the hazmat supply chain. (3.4) Tier 1 HSSM shippers and carriers, important external stakeholders in TSA's hazmat program, have workflow needs that the technology prototype did not meet. (3.10) The database supporting the technology prototype was not designed to support multiple user types, multiple business process workflows and the rich collaboration environment needed in a Tier 1 HSSM tracking program. (3.18) The technology prototype drew upon a limited set of data from external sources. (3.22)	**18. Build the truck tracking center to support efficient integration with DTTS, TRANSCOM and ACE.** • Integrate the Tier 1 HSSM truck tracking electronic manifest with the Custom and Border Protection truck e-manifest. • Build an interface with DTTS to bring data on military munitions shipments into the truck tracking system. Similarly, build an interface with DOE's shipment tracking system.
The technology prototype lacked sufficient system security. (3.28)	**19. Build a strong security infrastructure for the truck tracking system.** • Build a security infrastructure to protect business confidential and security sensitive information. • Build a desktop for a network security specialist.

Appendix A
TSA Universal Communications Interface

1. Universal Communications Interface - Interface Control (Version 1.6)

http://www.tsa.gov/assets/doc/universal_interface_control_document.doc

This document provides the details to enable a commercial truck tracking system to implement the non-proprietary universal interface set of protocols that enable the transmission of data from all commercially available tracking systems to the centralized truck tracking center.

- Section 2 identifies the Government and non-Government specifications and standards that apply to this system specification.
- Section 3 describes the implementation of the universal communications interface.
- Section 4 contains sample universal interface messages.

2. Universal Communications Interface - Interface Requirements Specification (IRS) (Version 1.5)

http://www.tsa.gov/assets/doc/universal_interface_requirements_specification.doc

This document specifies the requirements for implementing a centralized truck tracking center and for creating a non-proprietary UCI set of protocols to enable the transmission of data from all commercially available tracking systems to the centralized truck tracking center.

- Section 2 defines the requirements for the UCI.
- Section 3 identifies the qualification provisions that will assure each requirement from section 3 is met.
- Section 4 specifies the requirements traceability.
- Section 5 contains a listing of all acronyms and abbreviations used, and their meanings.

Blank

Appendix B
TSA Tier 1 HSSM Security Action Items

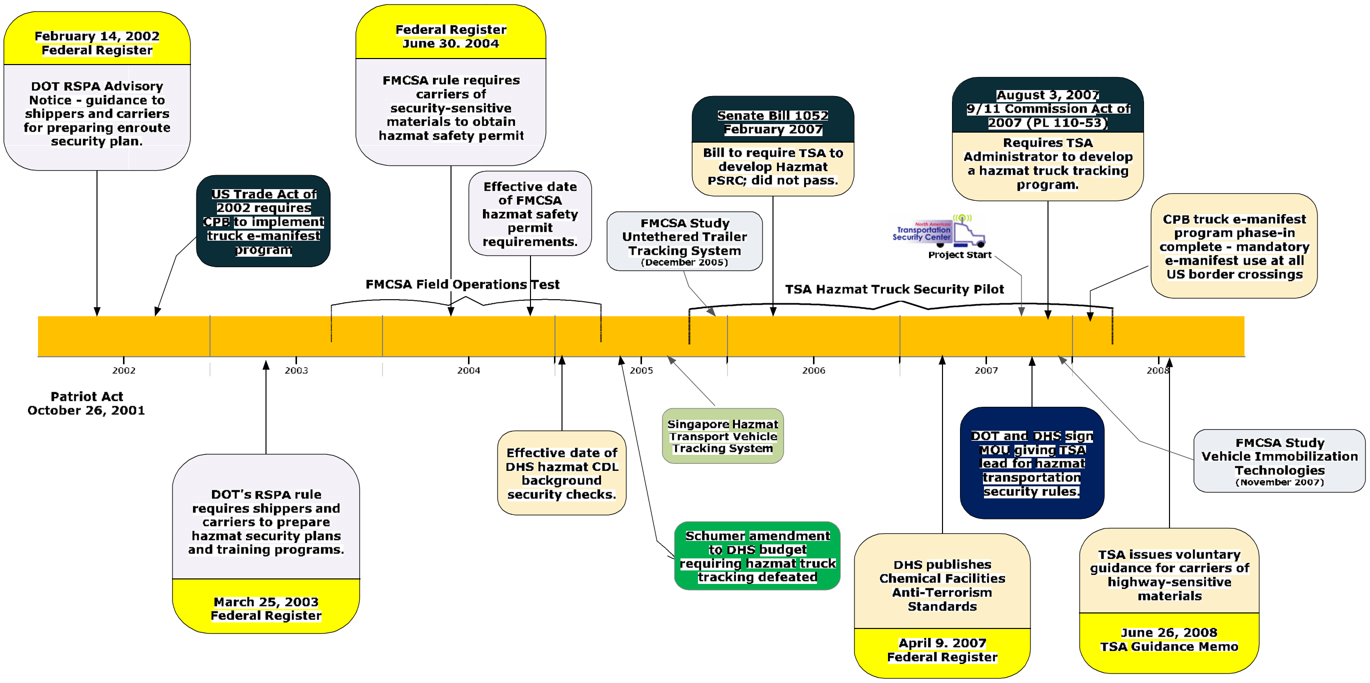
1.0 Hazmat security is driving the development of new regulations.

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

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

Figure B.1 presents a timeline of regulatory and legislative developments that affect hazmat shipment security. Sections 2.2 - 2.5 discuss the implications of these developments on the design and operation of the North American Transportation Security Center.

Figure B.1 Hazmat Security Regulations and Legislation Timeline



February 14, 2002
Federal Register
DOT RSPA Advisory Notice - guidance to shippers and carriers for preparing enroute security plan.
US Trade Act of 2002 requires CPB to implement truck e-manifest program
Federal Register
June 30. 2004
FMCSA rule requires carriers of security-sensitive materials to obtain hazmat safety permit
Effective date of FMCSA hazmat safety permit requirements.
FMCSA Field Operations Test
FMCSA Study Untethered Trailer Tracking System (December 2005)
Senate Bill 1052
February 2007
Bill to require TSA to develop Hazmat PSRC; did not pass.
North American Transportation Security Center
Project Start
TSA Hazmat Truck Security Pilot
August 3, 2007
9/11 Commission Act of 2007 (PL 110-53)
Requires TSA Administrator to develop a hazmat truck tracking program.
CPB truck e-manifest program phase-in complete - mandatory e-manifest use at all US border crossings
2002
2003
2004
2005
2006
2007
2008
Patriot Act
October 26, 2001
DOT's RSPA rule requires shippers and carriers to prepare hazmat security plans and training programs.
March 25, 2003
Federal Register
Effective date of DHS hazmat CDL background security checks.
Singapore Hazmat Transport Vehicle Tracking System
Schumer amendment to DHS budget requiring hazmat truck tracking defeated
DHS publishes Chemical Facilities Anti-Terrorism Standards
April 9. 2007
Federal Register
DOT and DHS sign MOU giving TSA lead for hazmat transportation security rules.
FMCSA Study Vehicle Immobilization Technologies (November 2007)
TSA issues voluntary guidance for carriers of highway-sensitive materials
June 26, 2008
TSA Guidance Memo

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

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

Transportation Security Administration

TSA has the lead responsibility for hazmat transportation security rulemaking.

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

The PHMSA also used the Federal Register notice to withdraw an Advanced Notice of Proposed Rulemaking (ANPRM) related to hazmat transportation security that the

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

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

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

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

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

Almost one year to the day that TSA formally assumed the lead federal responsibility for hazmat transportation security regulations, TSA issued guidance for shippers and carriers of highway security-sensitive materials. The guidance was issued by TSA's Assistant Administrator for Transportation Sector Network Management on June 26, 2008. [1] TSA's guidance recognizes two tiers of highway security-sensitive materials.

1. **Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM) –** HSSM transported by motor vehicle whose potential consequences from an act of terrorism include a **highly significant** level of adverse effects on human life, environmental damage, transportation system disruption, or economic disruption. A full list of Tier 1 HSSM may be found in **Appendix B**.

2. **Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)** - HSSM transported by motor vehicle whose potential consequences from an act of terrorism include **moderately significant** level of adverse effects on human life or health, environmental damage, transportation system disruption, or economic disruption. A full list of Tier 2 HSSM may be found in **Appendix B**.

3.1 TSA's security recommendations incorporate earlier DOT guidance.

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

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

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

TSA published Security Action Items (SAIs) for Tier 1 and Tier 2 HSSM shipments. SAIs are voluntary.

As illustrated in **Figure B.2**, TSA listed 23 Security Action Items (SAI) in its June 26th guidance. The SAIs are divided into four categories:

1. general security;
2. personnel security;
3. unauthorized access; and
4. en-route security.

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

Figure B.2 TSA HSSM Security Action Items

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

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

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

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.

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

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.

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

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

Security Action Item #19. Security for Trips Exceeding Driving Time under the Hours of Service of Drivers Regulation (49 CFR Part 395) – Employers should examine security in light of hours of service available and take steps to mitigate the vulnerabilities associated with extended rest stops for driver relief. Examples include methods such as constant vehicle attendance or visual observation with the vehicle, driver teams, or vetted companions. Other examples include arranging secure locations along the route through mutual agreement with industry partners and stakeholders, or

SAI #20 suggests that carriers should not subcontract or transload unless the subcontractor is security cleared.

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.

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

Security Action Item #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.

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

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

Figure B.3 lists Tier 1 HSSMs and the number of annual U.S. shipments of each HSSM.

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

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

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

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

Subject areas covered in the Act include homeland security and emergency management performance grants; communications interoperability; strengthening use of the incident command system; improving intelligence and information sharing and Congressional oversight of intelligence; preventing terrorist travel; privacy and civil liberties; private sector preparedness; improving critical infrastructure security; enhanced defenses against weapons of mass destruction; **enhancing transportation**

Figure B.3 TSA Tier 1 HSSMs

DOT Hazard Class	Hazmat Placard	Threshold Quantity	Number of Annual U.S. Shipments [2]
Division 1.1 Division 1.2 Division 1.3 Explosives	◆	Any quantity	Domestic - 11,868 NAFTA – 524
Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation)	◆	Anhydrous ammonia (UN1005) in single bulk packaging >300 L or 3000 kg	Domestic - 563,771 [3] NAFTA - 6,767
Division 2.3 Toxic (Poison) Gas Division 2.3 Toxic (Poison) Gas	◆	Hazard zone A & B >5lbs. in a single package Hazard zone C & D in single bulk packaging >3000L or 3000kg	Domestic - 960,871 NAFTA - 8,233
Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation)	◆	PG I in single bulk packaging > 3000 L or 3000 kg	Domestic - 62,015,889 [4] NAFTA - 119,816
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)	◆	Hazard zone A & B > 5 lbs. in a single package	Domestic - 307,244 NAFTA - 18,213
Division 6.1 Poisonous Materials (also meeting the definition of a material poisonous by inhalation)	◆	Hazard zone C & D in single bulk packaging > 3000 l or 3000 kg	
Class 7 Radioactive Materials	◆	IAEA Code of Conduct Category 1 and 2 materials including Highway Route Controlled quantities as defined in 49 CFR 173.403 or known as radionuclides in forms as RAM-QC by the Nuclear Regulatory Commission	Domestic - 7,777 NAFTA - 7,265
Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation)	◆	Packing group I and II in single bulk packaging > 3000 L or 3000 kg	Domestic - 4,548,595 [5] NAFTA - 95,703
Other Materials		Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules.	unknown
			Domestic – 1,287.760 [6] NAFTA – 34,235

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

[3] This figure includes shipments of Division 2.2 Non-Flammable Gases (subsidiary hazard Oxidizer Division 5.1) that are not inhalation toxic.

[4] This figure includes shipments of : 1). Class 3 Flammable Liquids (PGI and II in single bulk packaging > 300L or 3000 kg; and 2). Class 3 Flammable Liquids (any quantity desensitized explosives) – that are not inhalation toxic.

[5] This figure includes shipments of Class 8 Corrosive Materials (Packing group I in single bulk packaging > 3000L or 3000kg) which are not inhalation toxic.

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

security; preventing weapons of mass destruction proliferation and terrorism; international cooperation on security technologies; 9/11 Commission international implementation; and advancing democratic values.

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

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

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

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

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

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

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

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

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

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

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

UNITED STATES SENATE

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

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

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

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

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

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

In the October 2004 issue of *GPS World*, a leading trade magazine, the magazine's editor criticized ATA's opposition to GPS-based tracking systems for hazmat shipments as being disingenuous and short-sighted. [7]

> ***"...****Ironically, for years a rapidly growing number of trucking companies have been outfitting their fleets with just the kind of capability that ATA dismisses as an expensive, vulnerable, and cumbersome mandate, primarily because of the increased productivity that results.*
>
> *Of course, this is not the first instance of an industry resisting a security mandate. After 9/11, commercial airlines resisted some suggestions for methods of increasing security against terrorists, or argued that the government should pay for these measures. The dissenters usually have some credible reasons for not complying with the directive. Privacy. Cost. Bureaucratic burden. Inadequate preparation time. But the unspoken motive often seems to come from just not wanting to be obliged to do something.*
>
> *It brings to mind the closing stanza of Rudyard Kipling's poem, "The Lesson," composed in the wake of the disastrous Boer War: "We have forty million reasons for failure, but not a single excuse."*
>
> *Clearly, GPS is not a complete solution for the security needs of the U.S. transportation system. But just as clearly GPS should be a part of that solution. It's past time to make it so.* **"**

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

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

Editor - *GPS World*
October
2004

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

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

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

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

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

[7] *"Hazmat Keeps On Truckin',"* October 1, 2004, GPS World http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=126157

SECTION 1554. MOTOR CARRIER SECURITY-SENSITIVE MATERIAL TRACKING.

(a) Communications.--

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

Transportation Security Administration
Truck Security Pilot

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

(A) frequent or continuous communications;

(B) vehicle position location and tracking capabilities; and

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

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

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

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

(C) evaluate--

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

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

(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.

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

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

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

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

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

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

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

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

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

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

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

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

SEC. 1553. HAZARDOUS MATERIALS HIGHWAY ROUTING

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

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

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

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

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

(5) prepare guidance materials for State officials to assist them in identifying and reducing both safety concerns and security risks when designating highway routes for hazardous materials consistent with the 13 safety-based nonradioactive materials routing criteria and radioactive materials routing criteria in subpart C part 397 of title 49, Code of Federal Regulations;[8]

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

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

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

(b) Route Plans.--

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

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

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

electronic format, for explosives and radioactive materials. The assessment shall, at a minimum--

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

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

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

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

4.4 TSA plans to expand on the Hazmat Truck Security Pilot program.

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

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

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

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

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

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

- **Frequent or continuous communications** – TSA has developed a set of tested protocols that are capable of interfacing with (a) existing truck tracking systems, (b) state/local law enforcement agencies and first responders and (c) with federal intelligence and emergency management centers.

- **Vehicle position location and tracking capabilities** – TSA has implemented a tested and functioning truck tracking center that allows TSA to "continually" monitor truck locations and track load types in all of the continental United States.

- **A feature that allows a driver of such vehicles to broadcast an emergency distress signal** – TSA has developed a concept of operations that has gone through considerable testing and being vetted by government and industry volunteers. This concept of operations facilitates effective responses to drivers' emergency distress signals.

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

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

Blank

Appendix C
Truck Tracking Center Technology

XFML(Electronic) Forms

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

The Electronic Signatures in Global and National Commerce Act of 2000 enabled digital signatures/electronic forms to replace paper-based transactions.

Electronic (XFML) forms satisfy public and private digital business needs.[1]

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

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

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

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

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

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

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

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

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

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

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

E-forms create great value for organizations. For example, the U.S. Army is in the process of a large-scale project to convert its inventory of 100,000 forms used by 1.4 million people from a paper-based system to an e-forms system using IBM's Workplace Forms™ technology. Internal Army auditors estimate the Army will save $1.3 billion per year when the project is completed.[2]

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

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

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

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

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

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

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

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

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

Authorization can also occur at various places in an application. Most applications will require authorization for user login, document access, document submission, data queries, and so on. With the exception of user login, most of these authorizations are transparent to the user (single sign-on). Single sign-on systems can be extended to use within the context of the document itself. Document formats that support internal logic can make decisions regarding which sections of a document are available to the user. This is typically accomplished by server-side insertion of session sign-on information into the document or by embedding the document in HTML for portal use. The advantages of in-document authorization are mainly in the area of usability and error reduction. For example, sections of a paper form that are to be filled in by someone with manager credentials can be made read-only or invisible for someone without those credentials.

[2] http://www306.ibm.com/software/swnews/swnews.nsf/n/nhan6h9k99?OpenDocument&Site=lotus

This makes multi-stage documents significantly less error-prone, as well as easier for all users. In-document authorization can also allow for sensitive information to be contained in a document but not available to every user of that document.

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

Confidentiality - Who is allowed access to the document?

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

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

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

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

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

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

Business Rules Engines[3]

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

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

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

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

of these rules to IT applications that are affected or need to enforce one or more of the rules.

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

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

Business rules produce knowledge; work flows perform business work.

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

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

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

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

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

Most rules engines function as a callable library. However, it is becoming more popular for them to run as a generic process akin to the way that RDBMSs behave. Most engines treat rules as a configuration to be loaded into their process instance, although some are actually code generators for the whole rule execution instance and others allow the user to choose.

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

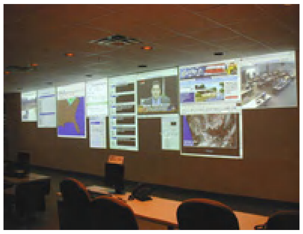
The other type of rule engine processes so-called reaction/Event Condition Action rules. The reactive rule engines detect and react to incoming events and process event patterns. For example, a reactive rule engine could be used to alert a watch officer that an unusually high number of dangerous hazmat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

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

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

Web-based crisis information management software supports “virtual” operations centers.[4]

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



Crisis information management software helps run emergency operations centers.

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

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

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

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

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

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