



# The North American Transportation Security Center -- Fedtrak Specifications and Release Plan

Report Number: KTC-19-33/FD05-1F

DOI: <https://doi.org/10.13023/ktc.rr.2019.33>



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

in cooperation with  
Kentucky Transportation Cabinet  
Commonwealth of Kentucky

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

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

in cooperation with  
Kentucky Transportation Cabinet  
Commonwealth of Kentucky

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

**Research Report**  
KTC-19-33/FD05-1F

**The North American Transportation Security Center – Fedtrak Specifications and Release Plan**

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.

July 2009

## Executive Summary

In April 2008, the **U.S. Transportation Security Administration** (TSA) completed work on the TSA Hazmat Truck Security Pilot (HTSP). This congressionally mandated pilot program was undertaken to prove that 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. In an earlier deliverable, the Kentucky Transportation Center (KTC) at the University of Kentucky examined the "gaps" between the HTSP technology prototype and an operational Tier 1 HSSM truck tracking system.

TSA needs a Tier 1 HSSM truck tracking system to support its regulatory ambitions, and FedTrak is being built to specifically serve as the implementing tool for TSA's Tier 1 HSSM regulatory program.

Deliverables 1.1 and 1.2 laid the foundation for development of the Specifications and Release plan for FedTrak, a Tier 1 HSSM truck tracking system. The Kentucky Transportation Center (KTC) held joint application design (JAD) sessions in Northern Virginia (June 3-5), in Lexington, KY (June 23-26) and again in Northern Virginia (July 15-16) to support development of the plan. A representative from NIHS attended the meeting in Lexington. This deliverable summarizes those meetings and the development approach the KTC project team will follow in building the FedTrak system. Specifically, this deliverable:

- summarizes specifications arising from project team JAD sessions (Section 1.2 and Appendix A);
- describes how "gaps" identified in Deliverable 1.2 will be filled (Section 1.1); and
- describes the FedTrak project team's architectural design and development approach (Sections 2, 3 and 4 ).

Release plans for the FedTrak shipper/carrier portals, the FedTrak electronic manifest application, and the FedTrak electronic route application are presented under separate cover.





# Table of Contents

<b>1.0 FedTrak Functional Specifications.....</b>	<b>1</b>
1.1 Deliverable 1.2 identified functional specifications for a Tier 1 HSSM truck tracking system.	
1.2 FedTrak project team meetings generated additional functional requirements.	
<b>2.0 Universal Communications Interface Refinements.....</b>	<b>33</b>
2.1 The original UCI was developed to support TSA’s HTSP Pilot program and is based on the IEEE-1512 messaging standard.	
2.1.1 Incident description message	
2.1.2 Resource assignment sub-message	
2.1.3 Cargo documents sub-message	
2.1.4 Cargo vehicle and cargo units sub-messages	
2.2 The FedTrak concept of operation calls for expanded UCI functionality but less dataflow through the UCI.	
2.2.1 Registration, electronic manifest, and routing applications will lessen the burden on the UCI and on fleet tracking vendors.	
2.2.2 The UCI will support 2-way system-to-system messaging between FedTrak and fleet tracking vendors.	
2.2.3 TSA may require the FedTrak UCI to support additional alerts and messages.	
<b>3.0 FedTrak Architecture.....</b>	<b>39</b>
3.1 The project team will use an integrated Microsoft/ESRI platform for development/operation of the FedTrak system.	
3.2 A commercial off-the-shelf business rules engine will support dynamic risk profiling.	
3.3 The building blocks of FedTrak are portals, applications, user desktops, and databases.	
<b>4.0 FedTrak Operational Scenarios.....</b>	<b>61</b>
4.1 Preparation of a trip plan for a Tier 1 HSSM shipment (carrier)	
4.2 Tier 1 HSSM shipment from “gate out” to “gate in” – no en-route shipment problems	
4.3 Risk score spike for en-route Tier 1 HSSM shipment (driver panic button)	

Appendix A - FedTrak Project Team Design Session Work Products

Appendix B– DOT/EPA Manifest Roles and Responsibilities



## 1.0 FedTrak Functional Specifications

This section presents the results of the analysis KTC conducted on the “gaps” between the functionality of TSA’s Hazmat Truck Security Pilot (HTSP) technology prototype and the functionality needed to support a Tier 1 HSSM truck tracking system.

It also summarizes project team meetings held in Northern Virginia (June 3-5), Lexington Ky (June 23-26), and again in Northern Virginia (July 15-16) in which the FedTrak project team developed FedTrak functionality requirements.

### 1.1 Deliverable 1.2 identified functional specifications for a Tier 1 HSSM truck tracking system.

After the FMCSA finished its Hazmat Safety and Security Technology Field Operational Test (FOT) in November 2004, Congress directed TSA to undertake the Hazmat Truck Security Pilot program. The purpose of the pilot program was to prove 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.

**Figure 1** presents a general schematic of a hazmat truck tracking center that KTC advanced in Deliverable 1.1. As indicated in Figure 1, six basic functional components – or core 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.

In late 2005 when the TSA HTSP began, there was a great deal of uncertainty about both technology and regulatory issues. The FMCSA’s Field Operations Test was completed a year before the HTSP 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.

Congress wisely chose to direct TSA to continue to build the programmatic infrastructure to support a hazmat truck tracking regulatory program by directing TSA to implement the HTSP program.

A significant challenges facing TSA in the HTSP program was enlisting a critical mass of hazmat carriers and fleet tracking vendors to support development of its hazmat truck tracking technology prototype. Even though the HTSP prototype’s functionality was



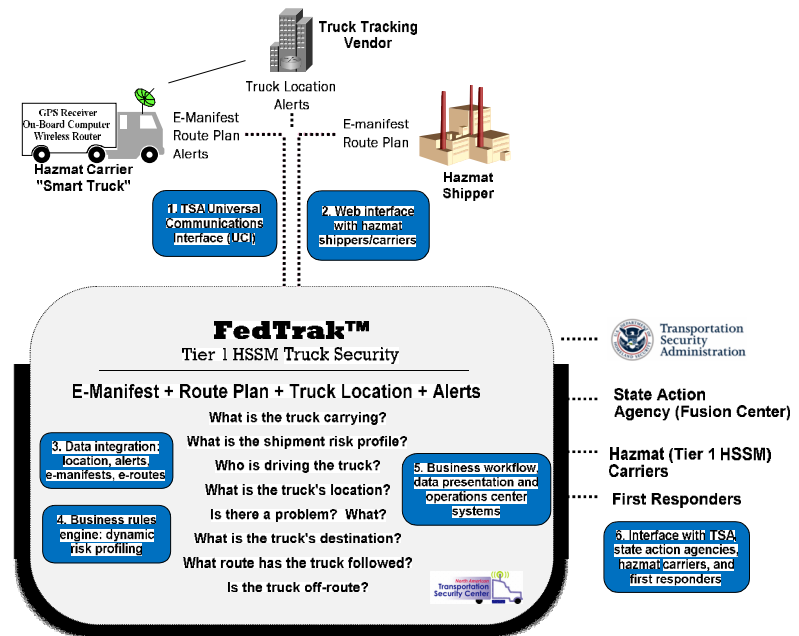
Congress directed TSA to undertake the Hazmat Truck Security Pilot project. TSA demonstrated that a truck tracking system is feasible from a technology and systems perspective.

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

Figure 1. Building blocks of a hazmat truck tracking center.

The core 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.



The HTSP project proved that a hazmat truck tracking center is feasible from a technology perspective. However, the HTSP technology prototype was not built to support a Tier 1 HSSM truck tracking program.

limited by industry participation, the HTSP pilot successfully proved 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.

However, the pilot fell far short of producing an operational system that would meet TSA's Tier 1 HSSM needs. NIHS Deliverable 1.2 examined the functionality "gaps" between the HTSP technology prototype and the functionality required by TSA in a Tier 1 HSSM truck tracking system. Deliverable 1.2 also listed recommendations for addressing the functional gaps. The results are presented in **Figure 2**.

Figure 2. Functionality gaps between the HTSP Technology Prototype and a Tier 1 HSSM truck tracking system.

Functionality Required in a Tier 1 HSSM Truck Tracking System	HTSP Technology Prototype Functional Gaps Addressed
<p><b>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 HSSM regulatory program based on TSA's Security Action Items.</b></p> <ul style="list-style-type: none"> <li>Design the tracking system to serve as the implementing tool for TSA Tier 1 HSSM regulations (Tier 1 HSSM SAIs). Functionality includes: <ul style="list-style-type: none"> <li>Vehicle tracking</li> <li>Untethered trailer tracking</li> <li>Vehicle immobilization</li> <li>Electronic route plans</li> <li>Electronic manifests (shipping papers)</li> <li>Route adherence monitoring</li> <li>Driver authentication</li> <li>Electronic locks/monitoring</li> </ul> </li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>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)</p> <p>The technology prototype did not deploy:</p> <ul style="list-style-type: none"> <li>an electronic route solution that will enable route adherence monitoring. (3.12)</li> <li>an untethered trailer tracking solution. (3.14)</li> <li>a vehicle immobilization solution. (3.15)</li> <li>an electronic lock/seal solution. (3.16)</li> </ul>

<ul style="list-style-type: none"> <li>○ Driver panic button/alerts</li> <li>• Full satisfaction of PL 110-53 requirements. Regulated parties (system users) will include Tier 1 HSSM shippers and carriers and fleet tracking vendors.</li> <li>• North American coverage; expected transaction volume about 2 million Tier 1 HSSM transactions/year.</li> </ul>	<p>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)</p>
<p><b>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.</b></p> <ul style="list-style-type: none"> <li>• Dataflow from carriers through the UCI should be restricted to vehicle location, gate out/in messages, and alerts from on-board sensors.</li> <li>• 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.</li> <li>• 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.).</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>The HTSP technology prototype relied too heavily on the Universal Communications Interface to bring data into the TEAMS application. (3.5)</p>
<p><b>3. Build portals with rich functionality for Tier 1 HSSM shippers and carriers; provide 24/7 access to corporate and shipment transaction data.</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Build portals to provide shippers and carriers access to shipment transactions: in-progress and completed.</li> <li>• Every shipper and carrier will have their own portal ("my portal"). Portals will allow company administrators to establish corporate user rights.</li> <li>• Build portals to allow shippers and carriers to complete system registration – i.e. load corporate data into the system database.</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>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)</p> <p>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)</p>
<p><b>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.</b></p> <ul style="list-style-type: none"> <li>• Merge information from the electronic manifest, the electronic route plan, vehicle location, and alerts to answer the following questions (see Figure 1.1). <ul style="list-style-type: none"> <li>• What is the truck carrying?</li> <li>• What is the shipment risk profile?</li> <li>• Who is driving the truck?</li> </ul> </li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>The technology prototype's alert notification and communications functions were degraded by architectural design flaws. (3.3)</p> <p>The technology prototype did not employ an electronic manifest solution that would allow it to efficiently accept load/driver/shipment information.</p>

<ul style="list-style-type: none"> <li>• What is the truck's location?</li> <li>• Is there a problem? What?</li> <li>• What is the truck's destination?</li> <li>• What route has the truck followed?</li> <li>• Is the truck off-route?</li> </ul> <ul style="list-style-type: none"> <li>• Deploy XFML technology (e-forms) to build an electronic manifest application to capture load information. Access via portal.</li> <li>• Build an electronic route preparation tool to support easy preparation/storage of carrier-defined routes. Access via portal.</li> <li>• E-manifest and e-route tools will draw on corporate data captured through registration.</li> <li>• Use latest GIS and portal (collaboration) tools to support development of the truck tracking center.</li> <li>• Build to efficiently process expected Tier 1 HSSM transaction traffic – 2 million transactions/year.</li> </ul>	<p>(3.6)</p> <p>The panic button business process workflow/system in the HTSP technology prototype did not work effectively and efficiently. (3.9)</p> <p>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)</p> <p>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)</p> <p>The prototype's design cannot effectively support the transaction volume expected in an operational system. (3.24)</p>
<p><b>5. Substantially expand the list of workflows/business processes served beyond those currently served by TEAMS.</b></p> <ul style="list-style-type: none"> <li>• The only business process addressed in the HTSP was the process associated with a driver panic button alert. The HTSP concept of operations was built around the actions that would be taken in the event of a panic button alert.</li> <li>• 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: <ul style="list-style-type: none"> <li>• An unauthorized driver attempts to pick up a Tier 1 HSSM shipment (SAI #6)?</li> <li>• A trailer is unexpectedly detached from a tractor during a shipment (SAI #23)?</li> <li>• A truck is substantially late or off-route of its expected route (SAIs #17,18)?</li> <li>• An electronic lock is breached during transit (SAI #13)?</li> </ul> </li> <li>• Workflows need to extend beyond the Security Specialist desktop to TSA. State fusion centers, emergency responders, etc.</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>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)</p> <p>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)</p> <p>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)</p> <p>The technology prototype did not deploy:</p> <ul style="list-style-type: none"> <li>• an electronic route solution that will enable route adherence monitoring. (3.12)</li> <li>• an untethered trailer tracking solution. (3.14)</li> <li>• a vehicle immobilization solution. (3.15)</li> <li>• an electronic lock/seal solution. (3.16)</li> </ul>
<p><b>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.</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>The technology prototype did not deploy an electronic route solution that will enable route adherence monitoring. (3.12)</p>

<ul style="list-style-type: none"> <li>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.</li> </ul>	
<p><b>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.</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Shippers/carriers can create and store electronic manifests on-line. They can retrieve them when needed to support a shipment.</li> <li>Electronic manifests must be submitted at or before "gate-out". Electronic manifests from completed transactions will be stored on shipper/carrier portals.</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>The HTSP technology prototype relied too heavily on the Universal Communications Interface to bring data into the TEAMS application. (3.5)</p> <p>The technology prototype did not employ an electronic manifest solution that would allow it to efficiently accept load/driver/shipment information. (3.6)</p> <p>The technology prototype did not support chain of custody monitoring of hazmat shipments. (3.13)</p>
<p><b>8. Scrap the geo-fencing approach used in the TSA HTSP; rebuild using upgraded GIS tools.</b></p> <ul style="list-style-type: none"> <li>Build a geo-fencing authoring tool using advanced GIS tools.</li> <li>Only authorized state and federal users will be allowed to create a geo-fence in the system.</li> <li>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.</li> <li>Geo-fences must be "reauthorized" periodically to avoid being purged from the tracking system.</li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>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)</p> <p>The prototype did not support variable location reporting frequency by hazmat carriers (2-way communication). (3.19)</p>
<p><b>9. Build the truck tracking center system to support untethered trailer tracking and vehicle immobilization.</b></p> <ul style="list-style-type: none"> <li>The UCI will be the path for alerts.</li> <li>Business rules risk scoring will likely push scores up high enough to require immediate attention of Security Specialists.</li> <li>Workflows specifically built for each scenario will support investigation/resolution by the Security Specialist.</li> </ul>	<p>The HTSP technology prototype was not built to support a Tier 1 HSSM regulatory program based on Security Action Item compliance. (3.1)</p> <p>The technology prototype did not deploy:</p> <ul style="list-style-type: none"> <li>an untethered trailer tracking solution. (3.14)</li> <li>a vehicle immobilization solution. (3.15)</li> </ul>
<p><b>10. Build desktops to meet the operational needs of personnel serving in the truck tracking center including security specialists and intelligence analysts.</b></p>	<p>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)</p>

<ul style="list-style-type: none"> <li>Security specialists will monitor shipments 24/7 and respond to issues arising with in-transit shipments.</li> <li>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.</li> <li>Other desktops might include a watch commander desktop and a user support desktop.</li> </ul>	<p>The technology prototype lacked intelligence analysis capabilities. (3.27)</p>
<p><b>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.</b></p> <ul style="list-style-type: none"> <li>Security specialists will likely use multi-screen workstations, and will need to be able to manage multiple incidents/issues at a time.</li> <li>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 should be able to initiate the call automatically from the desktop.</li> <li>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.</li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>The technology prototype's alert notification and communications functions were degraded by architectural design flaws. (3.3)</p> <p>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)</p> <p>The technology prototype only allows a security specialist to manage a single incident. (3.20)</p> <p>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)</p>
<p><b>12. Build a stand-alone business rules engine into the truck tracking center using a COTS software product.</b></p> <ul style="list-style-type: none"> <li>Use a powerful COTS business rules engine as a stand-alone tool – i.e. not integrated into a "black box" application.</li> <li>The business rules engine should be easy to modify "on the fly" by business analysts.</li> <li>Rule processing – especially alert processing - must be almost instantaneous.</li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>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)</p>
<p><b>13. Use the business rules engine to support dynamic risk profiling and to manage work load at the truck tracking center.</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>	<p>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)</p> <p>The technology prototype only allows a security specialist to manage a single incident. (3.20)</p> <p>The technology prototype is vulnerable to false positive which would overwhelm security specialists in an operational setting. (3.21)</p>

<ul style="list-style-type: none"> <li>Rules should always be tested before live loading to avoid overwhelming the truck tracking center with low priority alerts.</li> </ul>	
<p><b>14. Build 2-way communications capabilities between the truck tracking system and fleet tracking vendor systems to manage data reporting (variable reporting frequencies).</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Fleet tracking vendors' systems must be able to accept an automated request from the truck tracking center to adjust reporting frequency.</li> <li>For low-risk shipments in sparsely populated areas, reporting intervals &gt;&gt; 15 minutes may be sufficient. For high-risk shipments in sensitive areas, reporting intervals &lt; 15 minutes may be needed.</li> </ul>	<p>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)</p> <p>The prototype did not support variable location reporting frequency by hazmat carriers (2-way communication). (3.19)</p>
<p><b>15. Build an interface between the truck tracking center and state fusion centers to enable coordinated response to transportation security incidents.</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Collaboration must be efficient, fast, and easy. Automated or desk-top initiated communication will be a key feature of the Security Specialist desktop.</li> <li>Collaboration must flow through the state fusion center down to first responders in the field.</li> <li>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 through the state. The COP will feature a map visualization of in-transit shipments.</li> <li>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.</li> <li>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.</li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>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)</p> <p>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)</p>
<p><b>16. Build a NIMS-compliant communications infrastructure that will support efficient collaboration during a transportation security incident.</b></p> <ul style="list-style-type: none"> <li>Truck tracking center systems and business processes will be NIMS-compliant.</li> </ul>	<p>Outdated and/or underpowered tools (GIS, collaboration, web services) were used to build the HTSP technology prototype. (3.2)</p> <p>The concept of operations underlying the HTSP technology prototype was flawed and substantially</p>

<ul style="list-style-type: none"> <li>Extend business processes/workflows through the state fusion centers to emergency responders.</li> <li>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.</li> <li>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.</li> </ul>	<p>incomplete and did not reflect the critical role of states and other parties in securing the hazmat supply chain. (3.4)</p> <p>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)</p> <p>The HTSP technology prototype will not meet the operational needs of first responders. (3.25)</p> <p>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)</p>
<p><b>17. Build intelligence analysis capability into the truck tracking center.</b></p> <ul style="list-style-type: none"> <li>Build an intelligence analyst desktop to support the capability to anticipate and prevent security incidents.</li> </ul>	<p>The technology prototype drew upon a limited set of data from external sources. (3.22)</p> <p>The technology prototype lacked intelligence analysis capabilities. (3.27)</p>
<p><b>18. Build the truck tracking center to support efficient integration with DTTS, TRANSCOM and ACE.</b></p> <ul style="list-style-type: none"> <li>Integrate the Tier 1 HSSM truck tracking electronic manifest with the Custom and Border Protection truck e-manifest.</li> <li>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.</li> </ul>	<p>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)</p> <p>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)</p> <p>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)</p> <p>The technology prototype drew upon a limited set of data from external sources. (3.22)</p>
<p><b>19. Build a strong security infrastructure for the truck tracking system.</b></p> <ul style="list-style-type: none"> <li>Build a security infrastructure to protect business confidential and security sensitive information.</li> <li>Build a desktop for a network security specialist.</li> </ul>	<p>The technology prototype lacked sufficient system security. (3.28)</p>

## 1.2 FedTrak project team meetings generated additional functional requirements.

The FedTrak project team met in Northern Virginia (June 3-5) and in Lexington, Ky (June 23-26). Beginning with the gap analysis described in Section 1.1, the project team built an architectural schematic and working design specifications for the FedTrak system (presented in Section 2). The team also constructed a number of scenarios to describe how FedTrak will support operational situations that TSA would likely need to support in implementing its Tier 1 HSSM program (presented in Section 5).

The FedTrak project team expanded the functional specification list during project team meetings in Virginia and Lexington.

During its deliberations, the FedTrak project team generated lists of issues via a facilitated design session, and these issues have been factored into the FedTrak design specifications presented in Section 2. **Appendix A** contains snapshots of work product from the team's Lexington design session.

In addition, the project team captured a wide range of issues during its design sessions in Virginia and Lexington. These issues were useful in clarifying or expanding on the list of functional specifications described in Section 1.1 and in developing the FedTrak system specifications presented in Section 2. The issues/points captured by the project team covered a broad spectrum of the system design issues and include the following.

- **The FedTrak system development effort will lock with TSA's Tier 1 HSSM regulatory initiative.** FedTrak is being built as the implementing tool for TSA's Tier 1 HSSM regulatory program. While the framework for TSA's regulatory program is largely set with the adoption of the Tier 1 HSSM Security Action Items, TSA will be making refinements as it initiates formal rulemaking. FedTrak is being built to match Tier 1 HSSM SAIs, and will be refined as TSA proceeds with its formal regulatory initiative.
- **FedTrak registration is a one-time event.** FedTrak registration by Tier 1 HSSM shippers, carriers, and consignees will provide the system the information that FedTrak needs to support TSA's Tier 1 HSSM program. Registration will, however, be a one-time event for the parties. For example, during registration each shipper will be asked for corporate information including a listing of individuals that will be authorized to act on the shipper's behalf. FedTrak will also allow the shipper to designate the rights that individuals that work for the shipper will have in the FedTrak system. Upon conclusion of the registration process, each individual listed by the shipper will interact with FedTrak via their own personal portal. The individual's portal experience will reflect the individual's corporate type in FedTrak (ie shipper versus carrier or consignee) and the user rights that the shipper designated for the individual. The same registration process will be followed for carriers and consignees.
- **FedTrak will use the Standard Carrier Alpha Code as the key identifier for Tier 1 HSSM carriers.** The Standard Carrier Alpha Code (SCAC) will be the identifier for carriers in FedTrak. SCAC, a two-to-four digit identification, is used by the transportation industry to identify freight carriers in computer systems and shipping documents such as Bill of Lading, Freight Bill, Packing List, and Purchase Order. It is also used by the American National Standards Institute, Accredited Standards Committee X12, and United Nations EDIFACT for Electronic Data Interchange computer systems.
- **Tier 1 HSSM trading partners will establish business relationships during registration.** Tier 1 HSSM shippers, carriers, and consignees (trading partners) have business relationships that will drive the shipment transactions that FedTrak will monitor. The trading partners need to establish links that will underlie FedTrak's electronic manifest and electronic route applications. The following tables describe how shippers, carriers, and consignees will establish corporate affiliations in FedTrak. For example, during registration a shipper will be asked to provide a list of the Tier 1 HSSM carriers that the shipper uses. The shipper will use a carrier's SCAC in FedTrak for carrier identification. FedTrak will then facilitate the establishment of corporate affiliations between the shipper and the shipper's carriers. Establishment of a corporate affiliation between a shipper and carrier allows the parties to enter into electronic manifest transactions in Fedtrak.

FedTrak will be the implementing tool for TSA's Tier 1 HSSM regulatory initiative.

Tier 1 HSSM trading partners – shippers, carriers, and consignees – will establish corporate affiliations during registration that will allow FedTrak to support their Tier 1 HSSM business transactions.

The table below illustrates affiliation rights the trading partners will have in FedTrak. Note that FedTrak will allow carriers and consignees to request establishment of affiliations with shippers. For example, in the carrier's case the carrier will list its shipper customers during registration, and FedTrak will send a notice to each of the carrier's shipper customers registered in the FedTrak system. The shipper may approve or disapprove the carrier's request for a corporate affiliation. If the shipper approves the request, a business link is automatically established in FedTrak and the shipper-carrier can then enter into electronic manifest transactions.

Shipper	Carrier Affiliation
	<ul style="list-style-type: none"> <li>During registration, shipper lists carriers that provide Tier 1 HSSM cartage services to shipper.</li> </ul>
	<ul style="list-style-type: none"> <li>Carriers receive email alerting the carrier to the shipper's invitation for a corporate affiliation and asking the carrier to register/log onto FedTrak to accept the invitation.</li> </ul>
	<ul style="list-style-type: none"> <li>Carriers logs onto FedTrak portal and accepts shipper invitation. Corporate affiliation is complete. The shipper-carrier pair is authorized to enter into electronic manifest transactions in FedTrak.</li> </ul>
	Consignee Affiliation
	<ul style="list-style-type: none"> <li>During registration, shipper lists consignees to which the shipper provides Tier 1 HSSM shipments (ie those consignees for which the shipper wants a corporate affiliation).</li> </ul>
	<ul style="list-style-type: none"> <li>Consignees receive email alerting the consignee to the shippers's request for a corporate affiliation and asking the consignee to register/log into FedTrak to accept the request.</li> </ul>
	<ul style="list-style-type: none"> <li>Consignee logs onto FedTrak portal and accepts shipper's request. Corporate affiliation is complete. The shipper-consignee pair is authorized to enter onto electronic manifest transactions in FedTrak.</li> </ul>

Carrier	Shipper Affiliation
	<ul style="list-style-type: none"> <li>During registration, carrier lists shippers to which the carrier provides Tier 1 HSSM cartage services (ie those shippers for which the carrier wants a corporate affiliation).</li> </ul>
	<ul style="list-style-type: none"> <li>Shippers receive email alerting the shipper to the carrier's request for a corporate affiliation and asking the shipper to register/log onto FedTrak to accept the request.</li> </ul>
	<ul style="list-style-type: none"> <li>Shipper logs onto FedTrak portal and accepts carrier's request. Corporate affiliation is complete. The shipper-consignee pair is authorized to enter into electronic manifest transactions in FedTrak.</li> </ul>

Consignee	Shipper Affiliation
	<ul style="list-style-type: none"> <li>During registration, consignee lists shippers that provide Tier 1 HSSM products to the consignee.</li> </ul>
	<ul style="list-style-type: none"> <li>Shippers receive email alerting the shipper to the consignee's invitation for a corporate affiliation and asking the shipper to register/log onto FedTrak to accept the invitation.</li> </ul>
	<ul style="list-style-type: none"> <li>Shipper logs onto FedTrak portal and accepts consignee's invitation. Corporate affiliation is complete. The shipper-consignee pair is authorized to enter into electronic manifest transactions in FedTrak.</li> </ul>

- Serial numbers on fleet tracking equipment will be captured during registration.** When Tier 1 HSSM carriers register in FedTrak, they will be asked to

list the fleet tracking devices that will be on each truck, including serial numbers of each device. When a fleet tracking vendor sends a location or alert update to FedTrak via the UCI, the message will also include the device serial number. This allows FedTrak to link a message to a specific truck in the FedTrak system. It also lessens the burden on the UCI to send information about the truck/carrier with each UCI message.

- **FedTrak developers will consider using CAPTCHA during registration.** CAPTCHA is a type of challenge-response test used to prevent spammers from using computers to overwhelm a public facing application. Use of CAPTCHA should be considered for the public-facing FedTrak registration application. However, the registration process will not require system users to submit a registration request that requires human intervention/approval by FedTrak staff.
- **Shipper, carrier, and consignee administrators will establish user rights within their organizations.** FedTrak will support establishment of system user rights by corporate administrators. Some organizations will choose to manage their Tier 1 HSSM programs at the corporate level while others will choose to delegate responsibility down lower in the organization. Administrators will establish user rights based on defined roles. The table below illustrates user rights within a Tier 1 HSSM shipper organization. Note: individuals will likely play multiple roles. For example, one individual at a shipping location might serve as location administrator, shipment logistician, and shipment manager. FedTrak will also establish defined user rights for carriers and consignees.

Administrators will establish user rights within their organizations.

Roles	User Rights						
	Establish User Rights	Edit Corporate Data in FedTrak	Prepare Shipment for Transit	Prepare Electronic Manifest	Custody Exchange With Carrier	View En-Route Shipments	Respond to FedTrak Alerts & Inquiries
Tier 1 HSSM Shipper							
<b>Corporate Administrator</b>	Corporate-wide including other corporate administrators	<b>X</b> corporate wide	-	-	-	<b>X</b>	<b>X</b>
<b>Corporate Administrator (Subsidiary)</b>	Subsidiary-wide including other subsidiary administrators	<b>X</b> subsidiary wide	-	-	-	<b>X</b>	<b>X</b>
<b>Multi-Location Administrator</b>	Multiple locations including other multi-location administrators	<b>X</b> multiple locations	-	-	-	<b>X</b>	<b>X</b>
<b>Single Location Administrator</b>	Single location including other administrators at single location. Establish single location rights for all personnel at location.	<b>X</b> single location	-	-	-	<b>X</b>	<b>X</b>
<b>Pre-Transport Shipment Manager</b>	-	-	-	<b>X</b>	<b>X</b>	-	-
<b>Pre-Transport Shipment Logistician</b>	-	-	<b>X</b>	<b>X</b>		-	-
<b>En-Route Shipment Manager</b>	-	-	-	-	-	<b>X</b> Primary	<b>X</b> Primary

FedTrak will use electronic manifests as the mechanism to monitor chain of custody control of Tier 1 HSSM shipments.

FedTrak will leverage the work done by Customs & Border Protection by using ACE Truck E-Manifest data standards.

- **FedTrak will monitor Tier 1 HSSM shipment chain of custody.** FedTrak will use an electronic manifest application to monitor Tier 1 HSSM shipment chain of custody. The Tier 1 HSSM electronic manifest application will be similar in many respects to one that would support EPA hazardous waste shipments. However, EPA's programmatic objective is preventing illegal disposal while TSA is interested in preventing all or part of a Tier 1 HSSM shipment from being diverted while in transit and used as a weapon by a terrorist.
- **FedTrak's registration and electronic manifest applications will incorporate data standards/terminology developed for the Customs & Border Protection's ACE Truck E-Manifest system.** The ACE truck e-manifest program has developed five master sets of data elements that support e-manifest preparation.
  - Drivers
  - Conveyances (power units)
  - Equipment (trailers, containers, etc.)
  - Shipper
  - Consignee

FedTrak will adopt many of the ACE data elements for its registration and electronic manifest applications. Many of the ACE data elements related to corporate data will be collected during registration. This corporate data will be relatively static. Other data elements will vary for each manifest transaction, and will be collected at the time an electronic manifest is prepared.

The truck e-manifest has 70 data elements. Data elements (1) – (12) listed below are the core data elements for the truck e-manifest. Data elements (13) – (70) are included on the e-manifest as applicable. Those that are relevant to hazmat shipments are listed below. Notably, as illustrated in the table below, most of the data that will be included on a FedTrak electronic manifest will be collected during registration.

ACE Truck E-Manifest Data Elements	FedTrak	
	Collected During FedTrak Registration	Data Collected During Manifest Preparation
(1) Conveyance number, and (if applicable) equipment number (the number of the conveyance is its Vehicle Identification Number (VIN) or its license plate number and State of issuance; the equipment number, if applicable, refers to the identification number of any trailing equipment or container attached to the power unit. For purposes of this test, both the VIN and the license plate number are required);	<b>X</b>	
(2) Carrier identification (i.e., the truck carrier identification SCAC code (the unique Standard Carrier Alpha Code) assigned for each carrier by the National Motor Freight Traffic Association);	<b>X</b>	
(3) Trip number and, if applicable, the transportation reference number for each shipment (The transportation reference number is the freight bill number, or Pro Number, if such a number has been generated by the carrier.);		<b>X</b>
(4) Container number(s) (for any containerized shipment, if different from the equipment number), and the seal numbers for all seals affixed to the equipment or container(s);		<b>X</b>

(5) The foreign location where the truck carrier takes possession of the cargo destined for the U.S.;	<b>X</b>	
(6) The scheduled date and time of arrival of the truck at the first port of entry in the U.S.;		<b>X</b>
(7) The numbers and quantities for the cargo laden aboard the truck as contained in the bill(s) of lading (this means the quantity of the lowest external packaging unit);		<b>X</b>
(8) The weight of the cargo, or, for a sealed container, the shipper's declared weight of the cargo;		<b>X</b>
(9) A precise description of the cargo and/or the Harmonized Tariff Schedule (HTS) numbers to the 6-digit level under which the cargo will be classified.	<b>X</b>	
(10) Internationally recognized hazardous material code when such cargo is being shipped by truck;	<b>X</b>	
(11) The shipper's complete name and address, or identification number.	<b>X</b>	
(12) The complete name and address of the consignee, or identification number.	<b>X</b>	
(13) DOT number;	<b>X</b>	
(14) Person on arriving conveyance who is in charge;		<b>X</b>
(15) Names of all crew members;	<b>X</b>	
(16) Date of birth of each crew member;	<b>X</b>	
(17) Commercial driver's license (CDL)/drivers license number for each crew member;	<b>X</b>	
(18) CDL/driver's license State/province of issuance for each crew member;	<b>X</b>	
(31) Hazmat endorsement for each crew member;	<b>X</b>	
(42) Conveyance insurance company name;	<b>X</b>	

(43) Conveyance insurance policy number;	<b>X</b>	
(44) Year of issuance;	<b>X</b>	
(45) Insurance amount.	<b>X</b>	
(65) Hazmat contact.	<b>X</b>	

FedTrak will allow Tier 1 HSSM shippers and carriers to prepare electronic manifests. An electronic manifest application will be available via a portal.

- **Pick lists will make preparation of FedTrak electronic manifests quick and easy.** As the table above illustrates, most of the information needed on a Tier 1 HSSM electronic manifest will be collected as shippers, carriers, and receivers complete registration. Additional information needed to complete the manifest – such as the quantity of materials in the shipment – will be collected at the time of manifest preparation. **Shippers and carriers** will be able to prepare electronic manifests in FedTrak. FedTrak will allow carriers – specifically authorized by shippers – to prepare electronic manifests on behalf of their shipper customers.

Pick lists on the FedTrak manifest application will support quick and easy manifest preparation. Pick lists will be populated with corporate data collected via FedTrak registration. The table below describes the type of data that would be available on a pick list on a typical carrier's FedTrak portal site.

In this case, a Carrier is preparing an electronic manifest for a shipment from a Shipper to a Consignee. The parties have established corporate affiliations in FedTrak. When the Carrier selects the Shipper, the Carrier will be able to view and choose from a list of the Shipper's affiliated consignees. (Note: choosing shipment materials may modify the Consignee list as well if the Shipper ships different Tier 1 HSSMs to different Consignees.) The Carrier will select a Consignee from the pick list, as well as materials, driver, conveyance, equipment, and carrier contact. The Carrier can attach other documents such as Material Safety Data Sheets (MSDS) in an electronic envelope that will travel with the electronic manifest. The manifest will be complete when the preparer entered material quantity information including number of containers.

<b>Pick List Category</b>	<b>Information</b>
Shipper (shipping location)	Shipper name Shipping address Contact information
Consignee (receiving location)	Consignee name Receiving location address Contact information
Tier 1 HSSMs (specific list of materials in the shipment)	Hazmat name and descriptors
Driver	Name and identifying information including licenses
Conveyance	Information on the power unit the carrier will for the shipment.
Equipment	Information on the "smart truck" devices on the conveyance and trailer.
Carrier Contact	Name and contact information for the carrier contact for the shipment.
Electronic Envelope	Additional optional information the carrier elects to send along with the shipment.

- **FedTak will assign a unique identification number to each electronic manifest created in the system.** Each electronic manifest created in the FedTrak system will be assigned a unique identification number when it is first created.
- **Draft (work in progress) electronic manifests can be stored on the FedTrak system for up to 30 days; manifest templates will be stored indefinitely.** A shipper or carrier may create and store a "work in progress" or draft electronic manifest in FedTrak. This allows companies to preload FedTrak with draft electronic manifests that they want to use at shipment time. FedTrak will assign an identification number to draft electronic manifests. The system will purge draft manifests if the shipper or carrier does not use or modify them within 30 days.

A shipper or carrier may, however, store manifest "templates" indefinitely in the FedTrak system. A template captures information on regularly scheduled shipments from a shipper-consignee. Creation of a manifest template by a shipper/carrier is useful when very little information on the manifest changes from shipment to shipment. The only information that a standard template would not display would be driver and shipment quantity information. These are shipment-specific data elements that need to be entered into FedTrak at shipment time.

FedTrak electronic manifests will be easy to prepare – shippers and carriers have different options for preparing them.

- **FedTrak will allow a shipper/carrier to use a manifest from a prior shipment as a template for a new shipment.** FedTrak will allow a shipper/carrier to select a manifest from a completed shipment transaction as the starting point for creating a new manifest.
- **FedTrak will accept system-to-system electronic manifest uploads.** FedTrak will accept system-to-system manifest loading from corporate ERP systems or from shippers/carriers that use commercial software to support shipment logistics. FedTrak will publish XML schema that shippers/carriers can use to load manifest data into the FedTrak system. Note that this is similar in approach to the Universal Communications Interface in that system users will interact with FedTrak using published XML schema. This approach will be particularly useful to corporate users that wish to load many manifests in advance of scheduled shipments. Electronic manifests loaded into FedTrak will be managed as draft manifests by FedTrak.
- **Draft/template manifests created in FedTrak will be accessible by all the trading partners, however, only shippers and carriers will have edit rights for manifests stored in FedTrak.** Shippers and carriers have the right in FedTrak to create electronic manifests. Once created, all the trading partners associated with a manifest – including consignees - will be able to view it. Carriers and receivers will have edit rights for draft manifests stored in FedTrak.
- **The FedTrak registration and electronic manifest applications will be built using an XFML e-forms tool (Microsoft Infopath).** SERRI Section 3.6 described the value of forms in an organization as follows.

*"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."*

Microsoft's Infopath, an XFML electronic forms tool, will be used in the FedTrak electronic manifest application.

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).

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

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

Infopath (Microsoft's electronic form tool) will be at the heart of two major FedTrak applications – 1). the FedTrak registration application; and 2). the FedTrak electronic manifest application. Registration forms will be built using Infopath/Biztalk. Electronic manifest forms will also be built using Infopath/Biztalk.

Infopath supports the development of form-type applications for mobile devices, and FedTrak's electronic manifest application will be built so that drivers using mobile devices can access FedTrak via the internet and conduct electronic manifest transactions.

- **The FedTrak Tier 1 HSSM manifest form will have a similar "look and feel" to EPA's hazardous waste uniform national manifest form.** Hazardous waste is a subset of the much larger hazardous materials (hazmat) universe. EPA regulations require companies to track the movement of hazardous waste from the

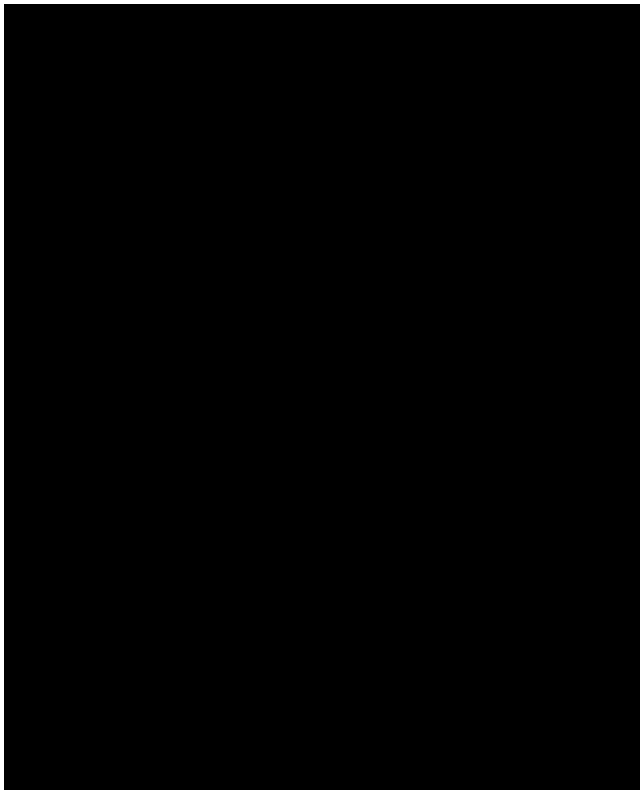
point of generation to the point of disposal ("cradle to grave") using a hazardous waste manifest form. There are about four million hazardous waste shipments in the United States each year.

EPA's manifest form – illustrated below - is a shipping paper/bill of lading tailored to meet the needs of the hazardous waste regulatory business process. It must accompany all waste shipments. The parties to the waste shipment (generators, transporters, receiving facilities) apply their signatures to the manifest form as custody of the waste shipment changes hands.

EPA's manifest form is broken into three sections. Section one is the generator's (shipper) section. Section two is the transporter's (carrier) section. Section three is the designated waste management facility's (consignee) section.

The generator's section includes information on the parties to the manifest transaction (generator, transporter, and facility) as well as information on the type and quantity of hazardous waste in the shipment.

The FedTrak manifest will look like EPA's hazardous waste manifest.



- **The FedTrak Tier 1 HSSM electronic manifest workflow will be similar to the EPA hazardous waste manifest workflow.**

EPA and DOT share regulation of hazardous waste shipments and DOT accepts EPA's hazardous waste manifest form in satisfaction of its shipping paper requirement (note: EPA's regulatory role does not extend to the hazmat universe beyond hazardous waste).

Currently, companies must use a multi-part paper hazardous waste manifest form. The use of paper manifests is cumbersome and expensive, and EPA plans to issue regulations that will allow companies to use electronic manifests instead of paper manifests for hazardous waste shipments. EPA's electronic manifest program will be built to meet the requirements of EPA's Cross Media Environmental Reporting Rule (CROMERR). Refer to **SERRI Section 2.6.3.1** and **Appendix A** for details. In general, an electronic manifest system must have the following functionality.

- Retain all the graphical elements familiar to the paper form. The manifests must be processed (prepared, signed, transmitted, and stored) in an entirely digital manner.
- Include non-line help features and edit checks to assist users with the process of completing the manifest accurately and quickly.
- Package form structure and data together in a single file that can be easily archived and retrieved.
- Integrate with workflow or work group software so that the manifests can be routed to appropriate trading partners, while complying with organizations' specific business processes and logic rules.
- Map directly to a variety of back-end data bases.

FedTrak electronic manifest business processes will be similar to those that will support a hazardous waste manifest program.

As parties to the e-manifest transaction sign the e-manifest, their portion of the form will be "locked" so that other parties cannot change the form later. As each e-manifest transaction takes place – such as a shipment chain-of-custody change – a 'snapshot' of the e-manifest form will be taken and stored in a database. E-manifest forms/transactions will be programmed to follow hazmat manifest business process workflow. For example, a load rejection by a consignee initiates a set of business processes that change the routing of the e-manifest form. Workflow events trigger notifications and on-line approvals and help connect Tier 1 HSSM shipper, carrier, and consignee business processes. E-mail is the communication mechanism for alerts.

The data elements on the FedTrak Tier 1 HSSM electronic manifest will differ somewhat from an EPA hazardous waste electronic manifest, however, the basic structure and function will be the same.

- **DOT allows carriers to prepare and sign shipping papers for hazmat shippers; EPA plans to adopt DOT's approach.** While there is some regulatory overlap between DOT and EPA, it is important to note that the two agencies operate off very different regulatory paradigms. DOT's hazmat regulatory focus is on maintaining the *safety* of hazmat shipments while EPA's regulatory focus is on maintaining waste shipment *chain of custody* to prevent illegal disposal. DOT places most of the responsibility for meeting its regulatory requirements on the hazmat carrier while EPA places most of its regulatory emphasis on the waste generator. Under EPA's regulatory view, a hazardous waste transporter is a passive party chosen by the generator to move waste from the generator to the generator's designated waste management facility. The generator retains full responsibility for ensuring that the waste shipment reaches its destination and is disposed of properly (e.g. full "cradle to grave" responsibility).

FedTrak will allow carriers to prepare and sign Tier 1 HSSM electronic manifests on behalf of a shipper.

DOT allows hazmat carriers to prepare shipping papers on behalf of shippers. EPA published a Federal Register notice March 4, 2005 describing its intent to modify its manifest requirements. Under EPA's revised approach, a transporter (carrier) could prepare and sign an electronic manifest on behalf of a generator (shipper). The March 4, 2005 Federal Register notice may be found in **Appendix A**. FedTrak will

allow a shipper to extend rights to a carrier to prepare and sign electronic manifests on the shipper's behalf.

Digital signatures on the FedTrak electronic manifest will support chain of custody monitoring.

- **The FedTrak electronic manifests will use digital signatures to promote document security and to support chain of custody monitoring.** SERRI Section 3.6 describes how digital signatures - integrated into an electronic forms application - will provide document security for business transactions. 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 authentication, authorization, confidentiality, and integrity.
  - Authentication - How do you know where the document came from?
  - Authorization - What permissions does the user have for working with the document?
  - Confidentiality - Who is allowed access to the document?
  - Integrity - How do you know if the document has been altered?
- **A shipper/carrier may attach an electronic envelope to a manifest.** FedTrak will allow shippers and carriers to append other documents and information to an electronic manifest. For example, the shipper/carrier may elect to attach Material Safety Data Sheets (MSDS) for the hazardous materials in the shipment. FedTrak will allow shipper/carriers to store lists of documents such as MSDSs on the site and select documents for individual manifests using a pick list mechanism.
- **A single shipment may have multiple electronic manifests and multiple consignees associated with it.** Most Tier 1 HSSM shipments will have only one Tier 1 HSSM on the truck and a single manifest for the shipment (one shipper, one manifest, one consignee). The entire shipment will travel from the shipper to a single consignee. However, shipments from a single shipper may have multiple manifests and multiple consignees (one shipper, multiple manifests, multiple consignees). The table below describes shipment situations with single/multiple consignees.

A single shipment may involve multiple manifests and multiple consignees.

Shipping Scenarios	One Tier 1 HSSM in Shipment	Two or more Tier 1 HSSMs in Shipment
<ul style="list-style-type: none"> <li>• Single Shipper</li> <li>• One consignee</li> </ul>	<ul style="list-style-type: none"> <li>• One manifest for entire shipment</li> </ul>	<ul style="list-style-type: none"> <li>• One manifest (more than one type of HSSM can be included on a single manifest)</li> </ul> <p style="text-align: center;"><b>OR</b></p> <ul style="list-style-type: none"> <li>• Multiple manifests if a manifest is prepared for each individual HSSM</li> </ul>
<ul style="list-style-type: none"> <li>• Single shipper</li> <li>• Two or more consignees</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple manifests - one for each consignee</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple manifests - at least one for each consignee.</li> </ul>

- **FedTrak will allow shippers to build a shipment containing both Tier 1 HSSMs and non-Tier 1 HSSMs.** Tier 1 HSSMs shipments represent a small percentage of the total number of hazmat shipments in the U.S. FedTrak will allow a shipper/carrier to build a shipment that contains both Tier 1 HSSMs and non-Tier 1 HSSMs. FedTrak will monitor the shipment as long as the shipment contains a Tier 1 HSSM.
- **Carriers are responsible for creating electronic route plans in FedTrak.** FedTrak will allow only carriers to create electronic route plans. Issue: some shippers will have a captive transport fleet, and will be recognized in FedTrak as both a shipper and carrier.
- **Carriers may build electronic route plans for their shipper-consignee paired customers and keep them on file in FedTrak.** As noted in a previous bullet, Tier 1 HSSM trading partners will establish corporate affiliations during registration.

Tier 1 HSSM carriers build route plans in FedTrak.

Shipper-consignee pairings will be established and the rights of a carrier to provide cartage services to a shipper will be established. FedTrak will allow an authorized carrier to build and store routes for the carrier's shipper-consignee pairs in FedTrak. As illustrated in the table below, a carrier may establish multiple routes for a given shipper-consignee pair. In this case, the carrier has built 2 routes from the Shipper A in Buffalo to Consignee X in Chicago and 3 routes from Shipper A to Consignee Y in Louisville. FedTrak will allow a carrier to build and store routes for all the carrier's shipper-consignee customer pairs. FedTrak will allow the carrier to build as many routes as desired for each shipper-consignee pair.

	Carrier's Stored Routes Shipper A/Consignee X Pair (Buffalo/Chicago, IL)	Carrier's Stored Routes Shipper A/Consignee Y Pair (Buffalo/Louisville, KY)
Shipper A (Buffalo NY)	Route 1 – rock star route <ul style="list-style-type: none"> <li>• I-80/I-90</li> <li>• Key waypoint - Cleveland</li> </ul> Route 2 – scenic route <ul style="list-style-type: none"> <li>• I-90/I-71/I-70/I-65</li> <li>• Key waypoints - Columbus; Indianapolis</li> </ul>	Route 1 – buckeye route <ul style="list-style-type: none"> <li>• I-90/I-71/I-64</li> <li>• Key waypoints – Cleveland, Columbus, Cincinnati Lexington</li> </ul> Route 2 – mountain route <ul style="list-style-type: none"> <li>• I-90/I-79/I-64</li> <li>• Key waypoints – Pittsburgh, Charleston, Lexington</li> </ul> Route 3 – I like Ohio route <ul style="list-style-type: none"> <li>• I-90/I-70/I-71/I-75/I-71</li> <li>• Key waypoints – Akron, Columbus, Dayton, Cincinnati</li> </ul>

- **FedTrak routing tools will make it easy to build route plans.** GIS tools will support fast, efficient construction of route plans. Carriers may enter shipper-consignee addresses into the routing tool, and FedTrak will construct a preliminary route. The carrier can "drag" the route to pass through the carrier's waypoint preferences. Once the carrier has established a shipper-consignee route, FedTrak will allow the carrier to store that route in the system for later retrieval as a preferred route for that specific shipper-consignee pair. FedTrak will allow a carrier to create and store xx (tbd) preferred routes for each shipper-consignee pair.
- **FedTrak will not allow a carrier to build a route plan that conflicts with DOT's National Hazardous Materials Route Registry.** The National Hazardous Materials Route Registry is the national repository of hazmat routes developed by DOT. Some of the routes in the registry are recommended routes for certain materials. Other routes in the registry are restricted routes.

FedTrak will not allow a carrier to build a route plan that conflicts with DOT restricted route registry.

FedTrak will not allow a carrier to create a route plan that conflicts with the registry.

Each route description within the registry contains the street, highway, bridge, or tunnel upon which the route is based and may contain two intersecting streets or highways (terminators) that define the starting and ending points of the route along the route. The route description also includes the following tags that identify what type of material is designated for transportation or restricted from use on the route.

Restrictions (Prohibited for the indicated hazmat)	Designations (Recommended for indicated hazmat)
0 - All Hazmats 1 - Class 1 - Explosives 2 - Class 2 - Gas 3 - Class 3 - Flammable 4 - Class 4 - Flammable Solid/Combustible 5 - Class 5 - Organic 6 - Class 6 - Poison 7 - Class 7 - Radioactive 8 - Class 8 - Corrosives 9 - Other i - Poisonous Inhalation Hazard (PIH)	A - All NRHM Hazmats B - Class 1 - Explosives I - Poisonous Inhalation Hazard (PIH) M - Medical Waste P - Preferred Radioactive Route

- **A carrier's route may involve stops at more than one consignee.** A carrier may stop at more than one consignee in a single trip. Tier 1 HSSMs would be on-loaded or off-loaded at each consignee. In FedTrak, the carrier will construct a route plan in which each consignee would essentially be a waypoint on the carrier's route. In the table below, the carrier's route would start at the shipper's location and have at least three waypoints – consignee A, consignee B, and consignee C.

Shipping Scenario	One HSSM in Shipment	Two or more HSSMs in Shipment	Route Segments
<ul style="list-style-type: none"> <li>• Single shipper</li> <li>• Three consignees – A,B,C - on single trip</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple manifests - one for each consignee</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple manifests – at least one for each consignee.</li> </ul> <p>(More than one type of HSSM can be included on a single manifest)</p>	<ul style="list-style-type: none"> <li>• Segment 1 – Gate Out Shipper to Gate In Consignee A</li> <li>• Segment 2 – Gate Out Consignee A to Gate In Consignee B</li> <li>• Segment 3 – Gate Out Consignee B to Gate In Consignee C</li> </ul>

- **A carrier will create a trip plan for a shipment from a shipper to a consignee by linking electronic manifests with the carrier's preferred routes for that shipper-consignee pair.** FedTrak will allow a carrier to build a trip plan by linking an electronic manifest with a route plan. The large majority of Tier 1 HSSM shipments will be a shipment of a single HSSM to a single consignee (the simple scenario below). However, FedTrak will support a more complicated scenario involving mixed loads, multiple manifests and multiple consignees.

**FedTrak Trip Plan**  
Route Plan + Electronic Manifest

A trip number will be assigned in FedTrak for each trip created by a carrier (ACE Truck E-Manifest consistency).

The table below describes how a carrier will build a trip plan in FedTrak.

Trip Plan = Route Plan + Electronic Manifest(s)		
	Simple Shipping Scenario	More Complicated Shipping Scenario
Number Manifests and Consignees	<ul style="list-style-type: none"> <li>• One Manifest</li> <li>• One Consignee</li> </ul>	<ul style="list-style-type: none"> <li>• Multiple Manifests</li> <li>• More than one type of Tier 1 HSSM on the truck</li> <li>• Three Consignees – A, B and C (see previous example)</li> </ul>
FedTrak Workflow for Creating Trip Plan	<ol style="list-style-type: none"> <li>1. Carrier logs onto FedTrak via carrier's portal and clicks on create trip plan button.</li> <li>2. Carrier selects originating shipper from pick list.</li> <li>3. Carrier selects shipper-consignee pair from pick list</li> <li>4. FedTrak displays pick list of draft or template manifests stored in system for the shipper-consignee pair; carrier selects manifest</li> <li>5. If a draft or template manifest is unavailable, FedTrak will prompt the carrier to build a manifest.</li> <li>6. Carrier selects a route from the carrier's preferred route pick list.</li> </ol>	<ol style="list-style-type: none"> <li>1. Carrier logs onto FedTrak via carrier portal and clicks on create trip plan button.</li> <li>2. Carrier selects originating shipper from pick list.</li> <li>3. Carrier selects multiple consignee trip option.</li> <li>4. Carrier selects Consignees A, B, and C from Shipper-Consignee Pair pick list.</li> <li>5. FedTrak displays pick list of draft or template manifests stored in system for each of the three shipper-consignee pairs. The carrier selects relevant draft/template manifests for each consignee.</li> <li>6. If draft or template manifests are unavailable, FedTrak will prompt the carrier to build manifests for the trip.</li> </ol>

	<p>7. If the carrier has not created a preferred route for the shipper-consignee pair, FedTrak will prompt the carrier to build a route for the trip.</p> <p>8. Carrier clicks complete, and Fedtrak creates and stores trip plan.</p>	<p>a. Manifest – shipper to Consignee A b. Manifest – shipper to Consignee B c. Manifest – shipper to Consignee C</p> <p>7. If carrier has created preferred routes for this group of Consignees, the carrier will select a route from the preferred route pick list.</p> <p>8. If the carrier has not created preferred routes for this group of consignees, the carrier will click on the Fedtrak routing tool and FedTrak will draw a route. The carrier will edit the route plan for specific preferences.</p> <p>9. Carrier clicks complete, and Fedtrak creates and stores trip plan.</p>
Trip Plan Contents	<p>1. Summary manifest page</p> <ul style="list-style-type: none"> <li>o Listing of high-level summary information from appended manifest form(s)</li> <li>o Map view of preferred shipper/consignee route selected by carrier from picklist on FedTrak</li> <li>o Turn by turn directions and listing of key waypoints</li> </ul> <p>2. Appended manifest form(s)</p>	<p>1. Summary manifest page</p> <ul style="list-style-type: none"> <li>o Listing of high-level summary information from appended manifest forms</li> <li>o Map view of preferred shipper/consignee routes <ul style="list-style-type: none"> <li>▪ Shipper to Consignee A</li> <li>▪ Consignee A to Consignee B</li> <li>▪ Consignee B to Consignee C</li> </ul> </li> <li>o Turn by turn directions and listing of key waypoints</li> </ul> <p>2. Appended manifest forms</p> <ul style="list-style-type: none"> <li>• Manifest form(s) for shipment to Consignee A</li> <li>• Manifest form(s) for shipment to Consignee B</li> <li>• Manifest form(s) for shipment to Consignee C</li> </ul>

- **FedTrak will allow a carrier to assign up to xx alternate routes that a driver may follow on a trip.** FedTrak will allow the carrier to assign alternate routes to a trip plan. FedTrak will allow a carrier to add up to xx alternate routes – alternate routes must branch off waypoints in the carrier's preferred route. Using a preferred route from the earlier example, the carrier will be able to add alternate routes on the stored route from Buffalo to Louisville. In the table below the carrier opted to create alternate routes branching off from the two established waypoints in the preferred route from Buffalo to Louisville. The waypoints branch points are Cleveland and Columbus. All roads eventually lead to Louisville from Buffalo, but the driver now has more options for getting there.

A carrier can establish alternate routes for a driver to follow in a trip plan.

	Carrier's Stored Routes Shipper A/Consignee Y Pair (Buffalo/Louisville, KY)	Alternate Route From Cleveland Waypoint  Modified Waypoint List	Alternate Route From Columbus Waypoint  Modified Waypoint List
Shipper A (Buffalo NY)	Route 1 – buckeye route <ul style="list-style-type: none"> <li>• I-90/I-71/I-64</li> <li>• Key waypoints – Cleveland, Columbus, Cincinnati Lexington</li> </ul>	<ul style="list-style-type: none"> <li>• Akron I-77</li> <li>• Canton I-77</li> <li>• Columbus I-70</li> <li>• Cincinnati</li> <li>• Lexington</li> </ul>	<ul style="list-style-type: none"> <li>• Dayton I-70</li> <li>• Cincinnati I-71 (I-71 to Louisville)</li> </ul>

For an en-route shipment, FedTrak will monitor the shipment location to ensure that it stays on the carrier's preferred route or one of the alternate routes filed with the carrier's trip report.

FedTrak begins to follow a Tier 1 HSSM shipment when a carrier applies a digital signature to an electronic manifest.

A carrier must file a trip plan in the FedTrak system before shipment "gate out".

FedTrak begins active tracking of a Tier 1 HSSM shipment at "gate out".

- **Shippers will verify driver credentials as part of the security process at the shipping location.** FedTrak will prevent a driver that is not registered in FedTrak from entering into an electronic manifest transaction with a Tier 1 HSSM shipper. FedTrak will not, however, provide a driver identity check service at the shipper/driver transaction point. TSA's SAIs urge shippers to implement pre-transport security programs. A critical step in the security process is an identity check of a driver by the shipper when custody of Tier 1 HSSMs shifts from shipper to driver (ie when the electronic manifest is signed). Shippers should inspect a driver's CDL to verify the driver's identity before entrusting custody of Tier 1 HSSM shipment to the driver.
- **Application of the carrier's digital signature on an electronic manifest at the shipper's facility will make the shipment "live" in the FedTrak system.** The custody of a Tier 1 HSSM shipment will shift from the shipper to the carrier when the carrier accepts custody of the shipment – signaled by the carrier's digital signature on the electronic manifest. FedTrak will recognize a shipment as an active shipment as soon as a digital signature on an electronic manifest is processed by the FedTrak system. Note that once the carrier applies a digital signature to the manifest, the shipper portion of the electronic manifest will be "locked". FedTrak will not allow any changes to the shipper's information – consignee identity, type/quantity of Tier 1 HSSMs – on a locked manifest.
- **A trip plan must be filed in the FedTrak system before shipment "gate out".** A carrier may not proceed to gate out at a shipper's facility until the carrier has filed a FedTrak trip plan. From an earlier bullet, a carrier will build a draft FedTrak trip plan for a shipment by linking two components – 1). the route plan for the shipment; and 2). electronic manifest(s) associated with the shipment. Associated manifests will not be in force until a carrier applies a digital signature to them signaling acceptance of custody of the shipment.

FedTrak will recognize a trip plan as final once the carrier has applied a digital signature to all the manifests associated with a shipment. A carrier may not proceed to "gate out" until a final trip plan has been filed in the FedTrak system. Note that Tier 1 HSSM carriers will likely be obligated to send a "gate out" signal to FedTrak via their fleet tracking vendor. If a "gate out" signal is received by FedTrak and there is not a corresponding trip plan for the shipment, the discrepancy will be noted by the system and flagged for action by a Security Specialist.
- **FedTrak will calculate a risk score for a shipment when the carrier files a final trip plan.** FedTrak's risk engine will calculate an initial risk score for a shipment when the carrier files a final trip plan for the shipment. At that point, the type/quantity of HSSMs is known and the route the driver will follow is known. Also, information on the shipper and consignee – including information on past shipments between them – can be factored into the scoring. The first update to the shipment risk score will be at "gate out".
- **The FedTrak system will initiate active shipment tracking when a truck reports "gate out" at a shipper's facility.** FedTrak will receive location reports on a truck from a carrier's fleet tracking vendor. FedTrak will begin to process location reports on a truck once that truck reports a "gate out" event at a shipper's facility. Tracking will continue until "gate in" at the consignee's facility.
- **A shipment risk score may change as a carrier drops off Tier 1 HSSM materials at a consignee's facility in a multi-consignee shipment.** As noted in a previous bullet, a carrier's trip plan may involve multiple consignees and multiple manifests. More than one type of Tier 1 HSSM may also be included in a shipment. As a carrier delivers HSSMs to successive consignees, the amount remaining on-board the truck will be less – likely reducing the risk profile for the shipment. With each delivery, FedTrak will recalculate the shipment risk score to account for the diminishing load amount and/or change in the mix of Tier 1 HSSMs on the truck.
- **FedTrak will monitor electronic manifest transactions/workflow.** As noted in a previous bullet, FedTrak will use an electronic manifest application to monitor Tier 1 HSSM shipment chain of custody. The Tier 1 HSSM electronic manifest application will be similar in many respects to one that would support EPA

hazardous waste shipments. Electronic manifest transactions/workflow will be constantly monitored to detect issues in the Tier 1 HSSM supply chain. FedTrak will monitor the following manifest transactions/workflow.

- Draft manifest filed in FedTrak
  - Manifest linkage to route (trip plan)
  - Carrier digital signature at shipper's facility
  - Load transfer from carrier to carrier (accident, mechanical problem)
  - Accident or spill (interruption in the supply chain)
  - Partial load rejection of a shipment by a consignee
  - Full load rejection of a shipment by a consignee
  - Shipment discrepancy exception report by consignee
  - Consignee signature at consignee's facility
- **FedTrak will monitor alerts (via fleet tracking vendors) that indicate unauthorized individuals are attempting to gain custody of Tier 1 HSSMs and will prevent unauthorized individuals from entering into a FedTrak business transaction.** TSA may require driver authentication requirements for carriers which involve smart card or biometric devices in the cab to prevent an unauthorized driver from operating a truck carrying Tier 1 HSSMs. FedTrak will monitor alerts from in-cab devices (via a carrier's fleet tracking vendor) to detect attempts by unauthorized drivers to take control of a Tier 1 HSSM shipment. FedTrak will also prevent a driver that is not properly registered in FedTrak to enter into an electronic manifest transaction with a shipper (i.e. assume custody of the Tier 1 HSSM shipment). Note that 'properly registered' in FedTrak means drivers must have a commercial driver's license with a hazmat extension.
  - **A carrier may file a modified trip plan in FedTrak for an en-route shipment.** During the course of an en-route shipment, a truck may need to be diverted from the planned route filed by the carrier due to weather conditions, road or traffic conditions, accidents, customer issues, etc. FedTrak will not register a system exception to a route change provided that the route change places the truck on one of the carrier's alternate FedTrak routes.

FedTrak allows a carrier to file an amended trip report while a Tier 1 HSSM shipment is en-route.

If the new route is not on one of the carrier's alternate FedTrak routes, FedTrak will allow a carrier to file an amendment to a trip plan for an en-route shipment that will allow the truck to follow a new route. However, a trip plan amendment will only be accepted in FedTrak if it is filed by an individual from the carrier's firm that has FedTrak administrator rights. FedTrak will not allow a driver to initiate an amendment to a trip plan to avoid the situation that the driver might be operating under duress.

- **The Universal Communications Interface (UCI) will be refined to support FedTrak.** The UCI was built during the TSA Hazmat Truck Security Pilot to allow fleet tracking vendors to feed data to a government truck tracking center. The UCI was based on the IEEE 1512 standard. Section 3 describes refinements that will be made to the UCI. In general, FedTrak portal applications (registration, electronic manifest, electronic route plan) will reduce the pressure on the UCI as a mechanism for data input from carriers/fleet tracking vendors. Additional functionality – most notably 2-way messaging between fleet tracking vendors and FedTrak – will be built into the UCI.
- **Application of the consignee's digital signature on an electronic manifest at the consignee's facility closes the transaction in the FedTrak system.** Three parties are listed on a manifest – the shipper, the carrier, and the consignee. FedTrak will monitor the chain of custody of Tier 1 HSSMs as a shipment moves from the shipper's possession to the carrier to the consignee. A carrier's digital signature on an electronic manifest signals FedTrak that the carrier has accepted custody of the shipment. In addition, a consignee's digital signature on an electronic manifest signals FedTrak that the consignee has accepted custody of the shipment. The consignee's digital signature also represents the close of a shipment transaction in FedTrak. Active shipment monitoring by FedTrak will cease and FedTrak will record the transaction as a completed transaction.

A consignee's digital signature on an electronic manifest closes the shipment transaction in FedTrak.

FedTrak will monitor untethered trailer alerts. Any disconnect between "gate out" and "gate in" will create an alert in the FedTrak system.

- **The FedTrak untethered trailer tracking (UTT) application will process tractor and trailer messages.** Commercial UTT systems have two sets of tracking/sensor devices – one for the tractor and one for the trailer. Data is reported to a fleet tracking vendor from both. Section 3.2 of *Deliverable 1.1 – SERRI Analysis Update*, described commercial UTT systems and how they work. During a Tier 1 HSSM shipment, the carrier's fleet tracking vendor will receive and pass location/alert data onto FedTrak from both the carrier's tractor and trailer.
- **A carrier will "link" a tractor and a trailer when the carrier prepares a trip plan for a Tier 1 HSSM shipment.** During registration, a carrier will register the serial numbers of installed "smart truck" devices on the carrier's tractors. Also, the carrier will register the serial numbers of UTT devices on the carrier's trailers. This allows FedTrak to "recognize" the UTT device when UTT data is reported to FedTrak by a carrier's fleet tracking vendor.

When the carrier builds a trip plan for a Tier 1 HSSM shipment, the carrier will specify the tractor and trailer that will be used in the shipment. This links the tractor/trailer pair for the pending shipment. Once the tractor/trailer are en-route, devices on both the tractor and trailer will report data/alerts to FedTrak via the carrier's fleet tracking vendor. FedTrak will know that the tractor and trailer are paired and will link the data from tractor/trailer units as it arrives. By linking the data, FedTrak will be able to detect an unanticipated trailer disconnect tractor/trailer between "gate out" and "gate in".

- **FedTrak will view trailer disconnects between "gate out" and "gate in" as an unauthorized event.** The objective of a UTT system is to detect unanticipated or unauthorized trailer disconnects. FedTrak will view a trailer disconnect between "gate out" and "gate in" as an unauthorized event and will flag the event for the attention of a Security Specialist. Note: a trailer disconnect at a consignee's facility in a multi-consignee shipment will not trigger the attention of the FedTrak system (shipment is not between "gate out" and "gate in").
- **"Follow me" systems will allow Security Specialists to find and contact a carrier hazmat contact.** On an electronic manifest, the carrier will list the firm's hazmat contact for the shipment. Presumably, that person will be available for consultation on a 24/7 basis if a problem with the shipment occurs. Realistically, the hazmat contact is often unavailable on a 24/7 basis. FedTrak will allow Carriers to use FedTrak "follow me" features to establish a "contact tree" keying off the listed corporate hazmat contact. If the person is unavailable for a telephone call, the call can be directed to follow the contact to a different device or to reach the contact using a different method (email, text message, etc). Or, the call can be directed to a different person altogether that is authorized to take the call and provide guidance on behalf of the carrier.
- **FedTrak will support carrier efforts to reroute trucks carrying Tier 1 HSSMs when DHS raises the Threat Condition to red.** TSA SAI 14, High Alert Level Protocols, recommends that carriers establish alternatives to routine operations when DHS elevates the Threat Condition to red such as:
  - identifying secure locations to seek refuge;
  - or shipments exceeding 200 miles, identifying private sector or law enforcement escorts to provide increased vehicle security, surveillance, and communications between local law enforcement officials and the motor vehicle while en route; or
  - employing other appropriate security measures identified by the employer. (Examples of planning for secure locations include mutual agreements with industry partners and stakeholders or utilizing state weigh stations and inspection facilities that can provide law enforcement protection.)

FedTrak Security Specialists will have the system capabilities to support carrier efforts to reroute Tier 1 HSSM trucks on the road if DHS raises the Threat Condition to red.

- **FedTrak will monitor shipment estimated time of arrival.** Carriers will calculate an estimated time of arrival for a Tier 1 HSSM shipment when they prepare the trip plan. Events on the road will, however, conspire to make some shipments late. FedTrak will monitor late shipments. The issue is to make a distinction between a shipment that is late for the right reasons versus a shipment that is late because it has been diverted by bad elements. The FedTrak business rules engine will be programmed to assess the difference and to feed recommended action to Security Specialists based on risk assessment.
- **The FedTrak user community will have expect the FedTrak public facing user interface to meet commercial design standards.** FedTrak user interfaces will meet a high commercial standard for aesthetics. Efficiency and speed of use is critical to user acceptance.
- **FedTrak service offerings need to meet the needs of Tier 1 HSSM shippers.** Tier 1 HSSM shippers will be the largest FedTrak user group. FedTrak services and features will be built to specifically support the shipper user community.
- **Tier 1 HSSM drivers will have a FedTrak smartphone application that will support the driver's needs while on the road.** With the widespread use of "smart phones", internet access is widely available via a cell phone connection. In addition, drivers that work for trucking companies served by fleet tracking vendors have access to the internet via truck on-board computers and wireless modems.

FedTrak's public facing user interfaces will be developed to meet commercial design standards.

Tier 1 HSSM drivers will be able to download FedTrak Mobile™, an application for use on mobile cellular-based devices. FedTrak Mobile™ will allow a driver to:

- make final edits to an electronic manifest such as quantity/type of HSSM in the shipment while at the shipper location;
- apply digital signature to electronic manifest;
- send geo-coded panic alerts to FedTrak;
- signal gate out at shipper facility;
- signal gate in/out at consignee;
- signal gate in/out at safe harbor;
- send messages to FedTrak and/or trading partners;
- receive messages from FedTrak and/or trading partners.

A FedTrak mobile application will allow Tier 1 HSSM drivers to conduct business transactions in the field.

TSA may opt to require a 'smart phone' as part of a core technology suite required of Tier 1 HSSM carriers.

- **FedTrak will allow carriers and consignees to use a telephony application to apply a digital signature to an electronic manifest.** In some locations, it may not be possible to make an internet connection. FedTrak will have a telephony application that will allow carriers and consignees to digitally sign an electronic manifest using a land-line telephone.
- **The FedTrak operations center will include a number of Security Specialist workstations; the master display wall will be a dominant physical feature of the operations center.** The FedTrak operations center will monitor Tier 1 HSSM shipments on a 24/7/365 basis. The largest group of workers at the FedTrak operations center will be Security Specialists who will monitor and react to situations that arise during shipments. A standard Security Specialist workstation will have a multi-monitor desktop setup. A dominant physical feature of the operations center will be the master display wall.

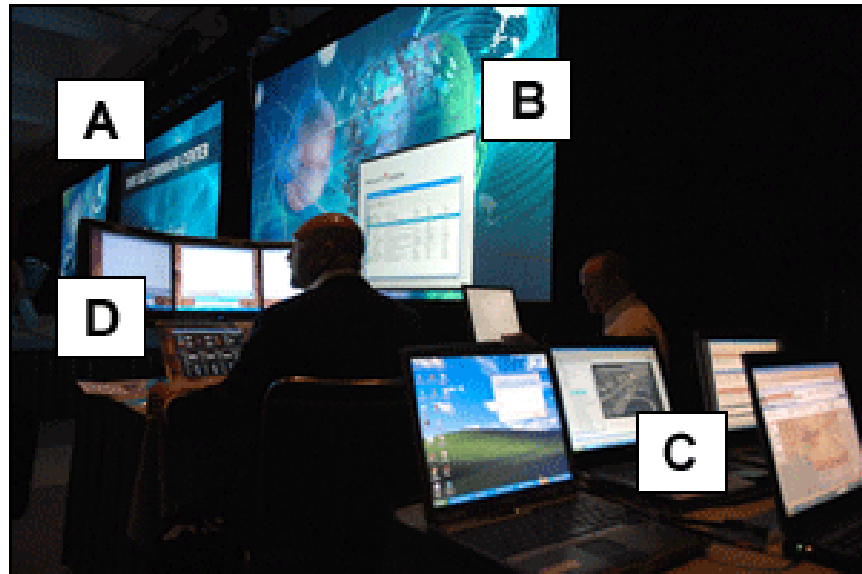
Carriers and consignees will be able to sign FedTrak electronic manifests using a telephone.

In October 2007, DHS Science & Technology Directorate demonstrated the use of COTS tools for Command and Control by using them to support a meeting at the January 2008 S&T Stakeholders Conference West.

DHS fused together a variety of technologies to create the DHS S&T COMMAND CENTER - a 1,000 person command briefing environment boasting 24.9 million pixels of information with the ability to show up to 36 simultaneous media sources in scalable, separate windows, all managed by a state-of-the-art advanced control

station. This command center is described below. Its operational components are consistent with those the project team expects to build into the FedTrak operations center.

#### **THE TECHNOLOGIES**



*The technologies that were brought together included:*

- A.** *A three-screen command wall with....*
- B.** *Extensive "source windowing" capabilities allowing....*
- C.** *Many computers and media feeds....*
- D.** *To be selected and displayed using a central command station*

*Using the command station, the different sources could all be accessed and displayed at-will as separate information windows placed anywhere on any of the screens.*

*Sources included: Computers with PowerPoint presentations; laptops linked into the Internet; live cameras; proprietary applications linked to restricted networks; and even live satellite links. Any of these could be arranged, sized and laid out into "screen sets" to be stored and recalled with simple mouse clicks. Sometimes sources were called for in real time and placed on the screens in response to events at the podium.*

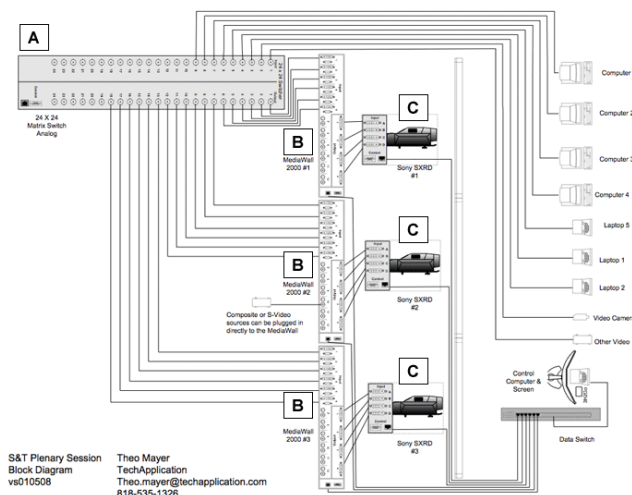
#### **THE BLOCK DIAGRAM**

*Many organizations spend months and even years planning and implementing a Command Center visual system. In this case, the leading edge, high performance and extremely flexible large-scale system needed to be transformed from "parts and pieces" into a fully functional command center in a day and a half. Good planning and a great technical team put up the basic system in a day. By noon the next day, we were rehearsing with a stabilized, reliable and fully operational command center.*

*In command center applications, all sources are typically linked into a matrix switcher (A) - a device that can take many video and audio inputs and send them to one or more outputs. The scale and complexity of this varies by facility and by mission.*

*Below, the outputs from the Matrix Switch (A) are directed into RGB Spectrum MediaWall 2000 units (B). These are the electronic image processors that allow sources to be placed into windows that can be sized, scaled, positioned, labeled, bordered, and more. The outputs of the MediaWall processors are sent to Sony's SXRD 4K projectors (C), each of which has an unprecedented 8.8 million pixel native resolution. This is ideal for command and control, since it allows all the pixels from a number of computers to be displayed at their full native resolution without shrinking or scaling the images down in order to fit the many windows onto the display.*

The FedTrak operations center will have a three-screen command wall.



RGB Spectrum MediaWall 2000 [www.rgb.com/en/Products/ViewProduct.asp?product=Mediawall2000](http://www.rgb.com/en/Products/ViewProduct.asp?product=Mediawall2000)

Sony 4K SXRD <http://bssc.sel.sony.com/BroadcastandBusiness/minisites/SXRD/visualization.shtml>

- **A FedTrak Security Specialist will have a multi-screen desktop.** FedTrak Security Specialists are responsible for monitoring en-route Tier 1 HSSM shipments. They will have a three-screen user interface.

FedTrak Security Specialists will have multi-screen desktops.

Screen 1 will display information on Tier 1 HSSM shipments in the Security Specialist's assigned regional area. A regional area may be a group of states, a single state, a metropolitan area, or any other geographic area. The FedTrak Watch Officer assigns areas to Security Specialists.

Screen 2 is the Security Specialist's workspace for evaluating Tier 1 HSSM shipments with high risk scores or for evaluating shipments of interest.

Screen 3 is reserved for shipments that trigger workflows that require collaboration with Tier 1 HSSM carriers/drivers, TSA, and/or state fusion centers. A shipment posted to Screen 3 will stay active until the workflow is complete and the issue causing the shipment to be posted to Screen is resolved.

Regional View Screen 1	Workspace Screen 2	Open Cases Screen 3
<ul style="list-style-type: none"> <li>• Messages and current statistics <ul style="list-style-type: none"> <li>◦ DHS Threat Level</li> <li>◦ Messages from Intelligence Specialist re: threats and "watch for" situations</li> <li>◦ Regional live statistics (dynamic) <ul style="list-style-type: none"> <li>◦ Number of Tier 1 HSSM shipments en-route on regional map</li> <li>◦ Score distribution of en-route shipments</li> <li>◦ Population at risk</li> <li>◦ Quick query/search tool – pick list of search criteria</li> </ul> </li> </ul> </li> <li>• <b>Map view</b> of area/region assigned to the Security Specialist <ul style="list-style-type: none"> <li>◦ Location of Tier 1 HSSM shipments</li> <li>◦ Locations of very important people, venues and events (temporal geo-</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Shipments with risk scores &gt;x on regional view automatically post to screen – cannot be overridden by Security Specialist or Watch Officer.</li> <li>• Some alerts – such as a driver panic alert - will always cause a shipment to post to the workspace and trigger a workflow that the Security Specialist must follow to completion.</li> <li>• A Security Specialist or the Watch Officer can set the system to post lower risk shipments to the workspace (ie post shipments with lower risk scores). The Watch Office can also set a lower risk score trigger for all Security Specialist desktops. A Watch Officer's trigger cannot be overridden by a Security Specialist.</li> <li>• Security Specialist may post any individual shipment (shipment of interest) from regional view screen to</li> </ul>	<ul style="list-style-type: none"> <li>• Displays up to 3 simultaneous cases for which FedTrak workflow requires external collaboration with carriers/drivers, state fusion centers and/or TSA. Screen landscape used as needed to manage multiple simultaneous cases.</li> <li>• Security Specialist or Watch Officer can move (assign) an open case to another Security Specialist's workstation.</li> <li>• All information and tools needed by a Security Specialist to resolve an open case is displayed on Screen 3.</li> <li>• Each open case follows prescribed workflow – Security Specialist is prompted step by step as the workflow unfolds.</li> <li>• An audit trail of a Security Specialist's actions and</li> </ul>

<p>fences)</p> <ul style="list-style-type: none"><li>o Map display parameters set by Security Specialist – ex. all shipments, material type, score &gt; than, all region area, state area, metropolitan area, location of established non-temporal geo-fences, critical infrastructure, hazmat, restricted routes, etc.</li><li>o Zoom in/out map function</li><li>o Roll over any map feature to drill down for additional information</li><li>• Map view covers Security Specialist’s assigned regional area. Contiguous regional areas are displayed on the Security Specialist’s map but in lighter screen tones in map view.</li><li>• List view of high score shipments and shipment status<ul style="list-style-type: none"><li>o List always sorts shipments by risk score – highest scores on top</li><li>o Maximum risk score 100.</li><li>o List information<ul style="list-style-type: none"><li>o Risk score and risk score acceleration rate</li><li>o Location (state, county, metro)</li><li>o Tier 1 HSSM type/quantity</li><li>o Reason(s) for inclusion (color codes)</li></ul></li><li>o The numbers of shipments included on the list is configurable by risk score – ie risk scores &gt;x will be displayed</li></ul></li><li>• Click-on feature to move shipment on map or list view to workspace screen.</li><li>• Messages and alerts - visual (flash, color) and auditory cues on map view and on list view highlighting shipments needing immediate attention</li><li>• Shipments with “look at me” scores automatically post to Security Specialist’s workup screen, the Intelligence Specialist Desktop, Watch Officer Desktop, and the master map</li></ul>	<p>workspace screen.</p> <ul style="list-style-type: none"><li>• Map view<ul style="list-style-type: none"><li>o Functionally similar to regional view</li><li>o View only those shipments automatically posted to workspace by FedTrak or selected for posting by Security Specialist</li></ul></li><li>• Shipment list view<ul style="list-style-type: none"><li>o Rollover any of the list items for additional information</li><li>o Click on any of the list items for detailed information</li></ul></li></ul> <table><tr><th>List Column Heading</th><th>Click-On Detailed Information</th></tr><tr><td>Shipper</td><td>tbd</td></tr><tr><td>Carrier</td><td>tbd</td></tr><tr><td>Consignee</td><td>tbd</td></tr><tr><td>Risk Score</td><td>Detailed breakdown of risk score  Lists risk score sub-components.  Narrative explanation of score.  Shipment risk score profile from gate-out and risk score acceleration rate during shipment.</td></tr><tr><td>Route</td><td>Displays shipment route followed.  Logs risk scores on map along route followed.  Other map information - tbd</td></tr><tr><td>Load</td><td>tbd</td></tr><tr><td>Quick Contacts</td><td>tbd</td></tr></table>	List Column Heading	Click-On Detailed Information	Shipper	tbd	Carrier	tbd	Consignee	tbd	Risk Score	Detailed breakdown of risk score  Lists risk score sub-components.  Narrative explanation of score.  Shipment risk score profile from gate-out and risk score acceleration rate during shipment.	Route	Displays shipment route followed.  Logs risk scores on map along route followed.  Other map information - tbd	Load	tbd	Quick Contacts	tbd	<p>communications during a workflow is stored in FedTrak operations database.</p> <ul style="list-style-type: none"><li>• Candidates for workflows that might be included in Screen 3 modeling.<ul style="list-style-type: none"><li>o Receive panic button alert from driver via in-cab device</li><li>o Receive panic alert from driver via smart phone (outside cab)</li><li>o Hijacking alert – shipment not secure, in-transit or unknown location</li><li>o Unauthorized driver attempts pickup</li><li>o Receive unexpected trailer separation alert.</li><li>o Receive equipment tampering alert</li><li>o Carrier loss of contact</li><li>o Accident notification – unknown result</li><li>o Accident – spill notification</li><li>o Off route – deviation from e-route plan (major)</li><li>o Off route – deviation from e-route; traveling on restricted route</li><li>o Off route – deviation from e-route plan (minor)</li><li>o Shipment exceeds ETA by xxx</li><li>o Unauthorized driver on-road with shipment – no hijack notice</li><li>o Gate out but no e-manifest and/or e-route plan filed</li><li>o Gate in message received – but wrong location</li><li>o DHS issues elevated (orange/red) threat level via the homeland security advisory system</li><li>o Action order/guidance from FedTrak Intelligence Specialist<ul style="list-style-type: none"><li>o SAR received – indicates possible security issue.</li><li>o TSA issues advisory based on specific parameters/criteria<ul style="list-style-type: none"><li>• Material type</li><li>• Shipper specific</li><li>• Carrier specific</li></ul></li><li>o Actionable intelligence from state/federal agency</li><li>o Actionable intelligence from shipper, carrier, or consignee</li></ul></li><li>o Secondary workflows (arise during the course of issue resolution)<ul style="list-style-type: none"><li>o TSA declares shipment of security interest.</li></ul></li></ul></li></ul>
List Column Heading	Click-On Detailed Information																	
Shipper	tbd																	
Carrier	tbd																	
Consignee	tbd																	
Risk Score	Detailed breakdown of risk score  Lists risk score sub-components.  Narrative explanation of score.  Shipment risk score profile from gate-out and risk score acceleration rate during shipment.																	
Route	Displays shipment route followed.  Logs risk scores on map along route followed.  Other map information - tbd																	
Load	tbd																	
Quick Contacts	tbd																	

		<ul style="list-style-type: none"> <li>○ TSA declares transportation security incident.</li> <li>○ TSA orders vehicle immobilization</li> </ul>
--	--	---

- **The FedTrak operations center will monitor about 2 million Tier 1 HSSM shipments per year.** At two million shipments per year, there will be about 5500 Tier 1 HSSM shipments/day in the U.S.

If 20% of Tier 1 HSSM shipments have a risk score high enough to warrant active monitoring, FedTrak Security Specialists will provide “eyes on” tracking of about 1200 shipments per day from “gate out” to “gate in”.

If 2% of the shipments trigger a Screen 3 workflow, Security Specialists will work on and resolve issues for about 100 shipments per day. If 5% of the shipments trigger a Screen 3 workflow, Security Specialists will work on and resolve issues for about 250 shipments per day.

- **The FedTrak Watch Officer will have a multi-screen desktop.** The FedTrak Watch Officer is responsible for the smooth operation of all Fedtrak operations. The Watch Officer’s desktop will be connected to all the following FedTrak desktops:
  1. Security Specialist Desktop
  2. Intelligence Specialist Desktop
  3. System Specialist Desktop
  4. Customer Service Desktop

The FedTrak Watch Officer will have a multi-screen desktop.

A FedTrak Watch Officer will be available to the TSA HQ contact(s) on 24/7 basis by telephone and internet to respond to any TSA HQ need for information or analysis of en-route Tier 1 HSSMs.

The Watch Officer desktop will have three screens.

Screen 1 will present the Watch Officer’s dashboard. At a glance, the Watch Officer will be able to get a reading on FedTrak operations and identify problems or issues needing attention. The contents and functionality of this screen will be developed in a later deliverable.

Screen 2 is the Watch Officer’s workspace. The Watch Officer will monitor workload and shift work between Security Specialists – the objective is an even distribution of work with no service gaps. The contents and functionality of this screen will be developed in a later deliverable.

Screen 3 is reserved for shipments that trigger workflows that require collaboration with Tier 1 HSSM carriers/drivers, TSA, and/or state fusion centers. The Watch Officer will monitor open cases and the resolution of cases. The contents and functionality of this screen will be developed in a later deliverable.

National/Regional Dashboard	Workspace	Open Cases and Post Resolution
tbd	tbd	tbd

- **The command wall in the FedTrak operations center will be configurable on-the-fly.** As noted in an earlier bullet, the master command wall in the FedTrak operations center will have three large screens onto which a variety of inputs can be displayed. The command wall will have one fixed screen that presents the common operating picture of Tier 1 HSSM shipments in the U.S. The other screens will be configurable to meet the needs of FedTrak operational staff.

DOT's Emergency Response Guidebook will provide FedTrak with data on hazardous materials.

- **FedTrak will have a North American service footprint and will need to provide trilingual service support (English, French, Spanish).** While FedTrak will primarily track shipments in the United States, some shipments will originate or end in Canada or Mexico. FedTrak will be built to serve the multi-lingual needs of its user community.
- **FedTrak will use DOT's Emergency Response Guidebook as the source for information on hazardous materials and response requirements.** The Emergency Response Guidebook (ERG2008) was developed jointly by the US Department of Transportation, Transport Canada, and the Secretariat of Communications and Transportation of Mexico (SCT) for use by firefighters, police, and other emergency services personnel who may be the first to arrive at the scene of a transportation incident involving a hazardous material. It is primarily a guide to aid first responders in (1) quickly identifying the specific or generic classification of the material(s) involved in the incident, and (2) protecting themselves and the general public during this initial response phase of the incident.

FedTrak will use the database underlying the ERG as its source of data for hazmat properties and hazmat incident response requirements.

The ERG is updated every three to four years to accommodate new products and technology. The next version is scheduled for 2012. The following URL provides a link to a video that describes the Emergency Response Guide and how it is used by hazmat first responders.

#### **Video 2008 Emergency Response Guidebook**

<http://www.phmsa.dot.gov/hazmat/library/erg>

ERG2008 Mobile is a software version of the ERG2008 featuring powerful search capabilities and a convenient, easy to use interface.<sup>1</sup> This software can be downloaded and installed on Microsoft Windows PCs and Windows Mobile PDAs/phones. A touch screen version is available for Windows Mobile devices.

- **FedTrak mobile applications will draw upon mobile applications built by the U.S. National Library of Medicine.** WISER (Wireless Information System for Emergency Responders) is a system designed to assist First Responders in hazardous material incidents.<sup>2</sup> Developed by the National Library of Medicine, WISER provides a wide range of information on hazardous substances, including substance identification support, physical characteristics, human health information, and containment and suppression guidance. WISER is available as a free standalone application on Microsoft Windows PCs, Windows Mobile devices, and Palm OS PDAs. Support for PDA-based browsers, including BlackBerry, is also available.

Wiser features include the following.

- Mobile support, providing First Responders with critical information in the palm of their hand.
- Comprehensive decision support, including assistance in identification of an unknown substance and, once the substance is identified, providing guidance on immediate actions necessary to save lives and protect the environment.
- Access to over 440 substances from NLM's Hazardous Substances Data Bank which contains detailed information on over 4,700 critical hazardous substances.
- Rapid access to the most important information about a hazardous substance by an intelligent synopsis engine and display called "Key Info".
- Visualization of protective distance zones on an interactive map.
- Radiological support, including radioisotope substance data, tools, and reference materials.
- Biological support, including biological agent data, tools, and reference materials.
- General tools, including an electronic version of the ERG.
- Intuitive, simple, and logical user interface developed by working with experienced first responders

---

<sup>1</sup> **ERG2008 Mobile Software Downloads** <http://www.phmsa.dot.gov/hazmat/library/erg#page6>

<sup>2</sup> **Wireless Information System for Emergency Responders** <http://wiser.nlm.nih.gov/index.html>

The WISER system concept is designed to work in a standalone or connected mode. The end user device is preloaded with the most critical information. At the scene, a wireless network sends new information between handhelds and routes requests for more information. If a wireless connection is not available, the handheld device still has full functionality with access to the critical local data available on the device.

WISER also sends and receives information over the wide area wireless network, receiving new information from dispatch, HSDB, or other sources.

A key feature of WISER is the support for identifying an unknown substance. WISER can help a First Responder identify and validate the unknown substance based on the following:

- sign/symptoms of victims of exposure
- physical properties of the substance gathered by observation or sensors
- hazard values from NFPA 704 placards
- the ability to categorize a substance, such as a substance used in a meth lab, a flammable substance, etc.
- transportation identification, including DOT placards, type of road trailer, and type of rail car

WISER allows the user to specify one of three roles they are currently performing at the scene. Information is presented to the First Responder, Hazmat Specialist, and EMS Specialist in the order that is most relevant to their respective role.

<b>First Responder</b>	<b>Hazmat Specialist</b>	<b>EMS Specialist</b>
Personal Protection Equipment	Physical Properties Summary	Treatment
Protective Distance	Personal Protection Equipment	Health Effects
Fire Procedures	IDLH (Immediately Dangerous to Life or Health)	Toxicity Summary
Reactivities	Flammability Limits	IDLH
Treatment	NFPA 704 Classification	NFPA 704 Classification





## 2.0 Universal Communications Interface Refinements

The HTSP Universal Communications Interface (UCI) is based on a web service that utilizes a federally endorsed XML messaging standard, the IEEE-1512. In the HTSP technology pilot, the UCI was developed as the chief mechanism for supplying a truck tracking center with the data it needs to function.

After the conclusion of the HTSP program, the KTC project team evaluated the HTSP UCI experience (see Deliverable 1.2 Technology Prototype Gap Analysis). The KTC SERRI project team recommended the following.

- FedTrak should retain the protocols/schema underlying the UCI developed for the HTSP. However, the UCI's role as the sole mechanism for loading data into TSA's truck tracking center should change. Other routes for dataflow (registration, e-manifest, and e-route applications) should be employed to complement the UCI as a data source for the truck tracking system.
  - 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 load or route information.
  - 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.). Do not use the UCI as the mechanism to capture corporate information for a particular shipment.
- Build 2-way communications capabilities between the truck tracking system and fleet tracking vendor systems to manage data reporting (variable reporting frequencies) and other messaging needs.
  - 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.
  - Vehicle immobilization will require messaging from FedTrak to truck-based systems via a carrier's fleet tracking vendor
- Adopt ACE Truck E-Manifest data standards for FedTrak registration, electronic manifest and electronic routing applications, but seek to build FedTrak XML interfaces using the IEEE-1512 XML standard.

### 2.1 The original UCI was developed to support TSA's HTSP program and was based on the IEEE-1512 XML messaging standard.

The HTSP required a non-proprietary universal interface or set of communication protocols that could enable the secure communication of information from truck tracking vendors. To accomplish this, the HTSP contractor used a web service based on the IEEE-1512 XML messaging standard.

The use of a web service provided an interface to anyone with internet access, satisfying the requirements of making the interface available to commercial truck tracking vendors. Data security requirements were met by communicating over secure

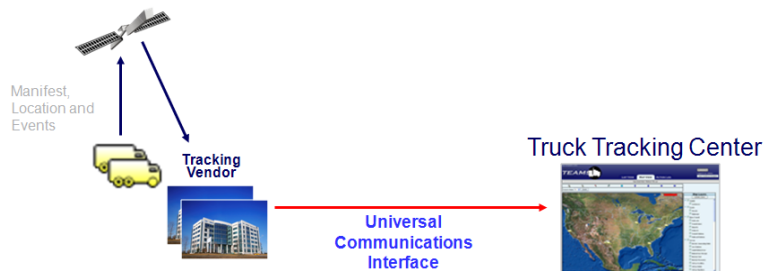


A Universal Communications Interface (UCI) was built during TSA's Hazmat Truck Security Pilot program as served as the interface with fleet tracking vendors.

The KTC project team made recommendations for refinements to the UCI.

sockets layer (HTTPS). HTTPS provides mutual authentication and data encryption. Additional security was provided by not embedding the UCI schema within the Web Services Definition Language (WSDL) file. By doing this, even if a username and password were comprised, an intruder still could not send a valid message to the centralized truck tracking center unless they had access to the schema.

IEEE-1512 provided an XML standard capable of representing all of the TSA-required data in a federal government endorsed standard. For the HTSP, messages from the IEEE-1512 base standard and IEEE-1512.3 standard were used. The use of IEEE-1512 requires a primary message and at least one sub-message for each data transmission. The base standard provided the primary message and 1512.3 provided the detailed sub-messages. For the HTSP the UCI was a one-way interface from the tracking vendors to the centralized truck tracking center.



To understand the use of the UCI for the HTSP requires understanding the event based approach used in the pilot. Each shipment from "gate out" to "gate in" was considered an event. When a vehicle departed with a shipment, the driver was expected to indicate a "gate out". This indication generated a UCI position report, which included the location, cargo manifest information and truck identification information. As the shipment progressed, periodic UCI position reports were generated to provide updates on the vehicles location. When the vehicle reached its destination, the driver provided a "gate-in" indication. This indication generated a final position report for the event. If an alert occurred during the course of the event, such as the driver pressing a panic button, a UCI message was immediately generated that reported the location of the vehicle and the reason for the alert.

### 2.1.1 Incident description message

The primary IEEE-1512 message used for all UCI transmissions was the 'Incident Description', or IDX, message. The IDX message provides the high level information required of all events. This information includes:

- Event ID – A unique ID used to identify a particular event
- Timestamp – The date and time that the message was sent
- Event Type – The reason for the message (i.e. position report, panic button press...)
- Location – The reported location of the event.

### 2.1.2 Resource assignment sub-message

Truck tracking data was provided by the 'Resource Assignment' sub-message. The 'Resource Assignment' sub-message provides:

- Unit ID – The ID of the vehicle being tracked
- Origin Location – The gate-out location of the vehicle

The HTSP UCI conforms to the IEEE-1512 XML messaging standard.

The IEEE-1512 Incident Description message provides high level information for a hazmat shipment.

The IEEE-1512.3 resource assignment sub-messages provide basic truck tracking data for a shipment.

- Current Latitude/Longitude – The reported location of the vehicle
- Destination Location – The anticipated gate-in location for the vehicle

### 2.1.3 Cargo documents sub-message

Cargo manifest information was provided by the Cargo Documents sub-message. The 'Cargo Documents' sub-message provides:

- Cargo Unit ID – A link to an identifier used to describe the cargo unit(s) transporting the material
- Vehicle Unit ID – A link to an identifier used to describe the power unit(s) transporting the material
- Shipper Name and location
- Carrier Name and location
- Shipment ID number – A unique number used to identify the shipment
- For each material being shipped:
  - Material ID number – UN/NA material identification number
  - Proper shipping name – The USDOT assigned name for the material
  - Hazard class/division – The hazard class and division for the material
  - Packing group – The packing group of the material
  - Quantity and units – The amount of the material being shipped

The cargo documents sub-message describes cargo manifest information.

### 2.1.4 Cargo vehicle and cargo units sub-messages

The vehicle being used for the shipment can be described by using one or more sub-messages. The 'Cargo Vehicle' message can be used to describe a power unit or a power unit in combination with cargo units. The 'Cargo Unit' sub-message can be used to describe un-tethered cargo units or detailed cargo containers. The 'Cargo Vehicle' sub-message provides the following data:

- Unit ID – The ID of the vehicle, as known by the carrier
- Vehicle Identification information, including:
  - Registration information
  - License plate information
  - Vehicle make
  - Vehicle color
- Driver Identification, including:
  - Driver name
  - Driver licensing

The vehicle being used for the shipment can be described by using one or more sub-messages (cargo vehicle sub-message and cargo units sub-message).

The 'Cargo Units' message provides the following data:

- Unit ID – The ID of the cargo unit, as known by the carrier
- Contents – The contents of the cargo unit, including:
  - Material ID number – UN/NA material identification number
  - Proper shipping name – The USDOT assigned name for the material
  - Hazard class/division – The hazard class and division for the material
  - Packing group – The packing group of the material
  - Quantity and units – The amount of the material being shipped

To describe the proper use of the UCI for commercial truck tracking vendors an Interface Control Document (ICD) was created. The ICD describes the use of each message and sub-message, and defines the contents of each. The ICD did not contain every

data element available within the UCI, instead including just those necessary to meet the requirements of TSA for the HTSP.

## **2.2 The FedTrak concept of operation calls for expanded UCI functionality but less dataflow through the UCI.**

FedTrak's concept of operation calls for more UCI functionality. For example, the UCI will be called on to serve as a 2-way messaging vehicle allowing the FedTrak system to send messages to fleet tracking vendor systems. Also, the existing UCI schema will be more fully used to support functions such as untethered trailer tracking. However, the FedTrak UCI will have a lower dataflow burden. Registration, electronic manifest, and routing applications will also feed data into FedTrak's Central Tracking Unit.

### **2.2.1 The FedTrak UCI will support 2-way system-to-system messaging between FedTrak and fleet tracking vendors.**

The FedTrak UCI will support 2-way, system-to-system communications with fleet tracking vendors.

The HTSP study concluded that a two-way communications interface between fleet tracking vendors and TSA's truck tracking center is needed, and that fleet tracking vendors should be required to automatically increase vehicle location reporting when directed by truck tracking center systems. This would involve a system-to-system messaging mechanism in which FedTrak would – based on the need for more frequent reporting – prompt a fleet tracking vendor's system to increase reporting frequency for a specified amount of time. This imposes a requirement on the fleet tracking vendor to have the capability to respond automatically to the FedTrak system (e.g. no human intervention).

A new UCI message, the 'Reporting Frequency Message' will be a system-to-system message that will prompt a fleet tracking vendor's system to increase or decrease location reporting based on a truck's risk score.

FedTrak will be programmed to automatically issue a 'Reporting Frequency Message' via the UCI to a fleet tracking vendor's system based on a shipment's risk score. For shipments with high risk scores, FedTrak will send a fleet tracking vendor's system a 'Reporting Frequency Message' asking for more frequent location reporting. For shipments with low risk scores in less populated areas, FedTrak will send a fleet tracking vendor's system a 'Reporting Frequency Message' asking for much less frequent location reporting. Note that the FedTrak business rules engine will need to be programmed to support FedTrak's 'Reporting Frequency Message' mechanism.

The creation of the 'Reporting Frequency Message' is one of a number of new UCI messages types that may need to be created to support FedTrak needs. The project team will create new messages using the IEEE-1512 format and data frames. This will create more appropriately named messages that are directly meant to satisfy FedTrak requirements. For example, the primary message used for sending FedTrak messages would be the 'Request for Information' message. The basic structure of the 'Request for Information' message could be preserved, with the 'Reporting Frequency Message' serving as one of a number of sub-messages.

The FedTrak UCI will support FedTrak to driver messaging.

The FedTrak UCI will also support FedTrak-to-driver messaging on a vehicle's on-board computer or a driver's smart phone. IEEE-1512 provides a 'Description' message that is meant for the exchange of free text information. The 'Description' message provides the following information:

- Tracking device ID – The ID number of the tracking device on the vehicle being sent the message
- Subject – The subject of the message
- Description – The actual message being sent

The UCI will also be refined to support TSA vehicle immobilization requirements. The 'Immobilize Truck' message will be sent to a carrier's truck from FedTrak via the carrier's fleet tracking vendor. It would initiate vehicle immobilization by activating truck-based immobilization devices. Remote vehicle disabling systems provide authorized users at remote locations such as a fleet operations center the ability to prevent an engine from starting, prevent movement of a vehicle, and to stop or slow a moving vehicle. Remote disabling allows a dispatcher or other authorized personnel to gradually decelerate a vehicle by downshifting, limiting the throttle capability, or bleeding air from the braking system from a remote location. Some of these systems provide advance notification to the driver that the vehicle disabling is about to occur. After stopping a vehicle, some systems will lock the vehicle's brakes or will not allow the vehicle's engine to be restarted within a certain timeframe. Refer to Section 3.3 of Deliverable 1.1 – "SERRI Analysis Update" for more detailed information on vehicle immobilization systems including a survey of available commercial systems.

The FedTrak UCI will support vehicle immobilization.

The 'Immobilize Truck' message will be a sub-message to the UCI's existing "Request for Information" message. The 'Immobilize Truck' message will contain the following information:

- Tracking device ID – The ID number of the tracking device on the vehicle that should be immobilized
- Event Type – A phrase indicating that an immobilization is being requested

#### **2.2.2 Registration, electronic manifest, and routing applications will lessen the burden on the UCI and on fleet tracking vendors.**

In the HTSP program, the UCI was the primary mechanism for feeding data to the truck tracking center. In FedTrak, other applications – notably registration, electronic manifest, and routing applications – will feed data into FedTrak. This will substantially lessen the burden on the UCI as a data transport vehicle, and will lower the data reporting burden on Tier 1 HSSM carriers.

The FedTrak UCI will not be the only mechanism for data flow into FedTrak.

The FedTrak project team expects to build electronic manifest and electronic route applications that will support uploads from corporate ERP systems. XML interfaces for these applications – like the XML interface that the UCI provides to fleet tracking vendors – will make manifest/route loading into FedTrak easy and efficient.

The FedTrak project team plans to use ACE Truck E-Manifest data conventions as it builds its registration, electronic manifest and routing applications. However, the project team will seek consistency with the IEEE-1512 XML messaging standards as it builds its manifest and routing applications. For example, a UCI sub-message, 'Route Advice', might be developed to provide the following data:

The FedTrak project team plans to build additional XML interfaces; will seek consistency with the IEEE-1512 standard.

- Route name
- Route origin
- Route components
- Route destination
- Estimated travel time

### **2.2.3 TSA may require the FedTrak UCI to support additional alerts and messages.**

TSA plans to implement a Tier 1 HSSM regulatory program based on its existing Security Action Items. These rules will bring with them requirements for Tier 1 HSSM shippers, carriers, and consignees that FedTrak will need to support. For example, FedTrak will likely need to support untethered trailer tracking. In this case, the 'Cargo Unit' sub-message can be used to describe un-tethered cargo units or detailed cargo containers.



### 3.0 FedTrak Architecture

This section presents the working design specifications developed by the project team during joint application design sessions in Lexington and Northern Virginia.

#### 3.1 The project team will use an integrated Microsoft/ESRI platform for development/operation of the FedTrak system.

FedTrak will leverage the investment made by Microsoft and ESRI in building the Fusion Core product. On July 13, 2009, Microsoft and ESRI introduced the Fusion Core product for State fusion centers. Fusion Core is a collaborative initiative between Microsoft and ESRI, the leading GIS software firm in the world. Fusion Core will allow State fusion center to integrate their existing data holdings to create actionable security intelligence.

FedTrak will leverage the Microsoft/ESRI investment in the Fusion Core product, a state fusion center tool.

Fusion Core has the following capabilities.

- o Data management and visualization capabilities, including Suspicious Activity Reporting.
- o Pre-loaded and customizable forms for processing, assigning, and satisfying many different types of intelligence and information service requests.
- o Tools to search across multiple data sources, including file shares, Web sites, and databases.
- o Powerful and extendable geospatial analysis capabilities.
- o Integrated capabilities that enable analyst and customer collaboration by using Web sites, blogs, and wikis.
- o Easily configured, secure connections to external data sources and supported connectivity to a Department of Homeland Security (DHS) Information Sharing Environment (ISE) Shared Space, eGuardian, and the Automated Critical Asset Management System (ACAMS).
- o Out-of-the-box functionality that can be integrated with existing authentication and auditing systems to enhance security.
- o Powerful management reporting capabilities.

At the heart of Fusion Core is an integrated Microsoft/ESRI software stack. It is the same software stack that will be used to support the FedTrak application.

FedTrak will be built using almost the identical software stack used in Fusion Core.

- o Office Performance Point Server 2007
- o SharePoint Server 2007
- o SQL Server 2008 Enterprise
- o Windows Server 2008 Enterprise
- o Office 2007 Professional
- o System Center Virtual Machine Manager
- o ESRI ArcGIS Advanced 9.3 Enterprise Server
- o ESRI ArcInfo 9.3
- o ESRI ArcGIS Explorer
- o ESRI 2D Viewer

FedTrak will leverage Microsoft's unified communications infrastructure to build efficiency and functionality into desktop operations. The communications infrastructure underlying the Security Specialist Desktop will be based on Microsoft unified communications technologies. The following video describes Microsoft's unified communications.

FedTrak desktop applications will leverage Microsoft's unified communications infrastructure.

<http://www.microsoft.com/uc/default.mspx>

The plan for building *FedTrak Connect* using Microsoft unified communications tools will be developed in a later deliverable

### 3.2 A commercial off-the-shelf business rules engine will support dynamic risk profiling

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

The FedTrak project team will incorporate a commercial-off-the-shelf (COTS) business rules engine into the FedTrak architecture.

### 3.3 The building blocks of FedTrak are portals, applications, user desktops, and databases.

Portals, databases, applications, and user desktops will be the building blocks of the FedTrak system.



FedTrak Architectural Components			
Portals	Databases	Applications	User Desktops
<ul style="list-style-type: none"><li>• Tier 1 HSSM shipper</li><li>• Tier 1 HSSM carrier</li><li>• Tier 1 HSSM consignee</li><li>• Fleet tracking vendor</li><li>• Government</li><li>• TSA HQ (Ed Bowers)</li><li>• State action agencies (Fusion Center)</li><li>• TSA Operations Center</li><li>• Tier1 HSSM driver (via carrier portal)</li><li>• Emergency responders (via fusion center portal)</li></ul>	<ul style="list-style-type: none"><li>• Geo-fence</li><li>• DOT restricted route registry</li><li>• Corporate data repository</li><li>• Shipment transaction repository</li><li>• FedTrak operations repository</li><li>• Shipper/carrier information</li></ul>	<ul style="list-style-type: none"><li>• Geo-fence builder</li><li>• Route builder</li><li>• Registration</li><li>• FedTrak central tracking unit (CTU)</li><li>• FedTrak risk engine</li><li>• FedTrak mobile applications</li><li>• FedTrak connect</li></ul>	<ul style="list-style-type: none"><li>• Security Specialist</li><li>• Intelligence Analyst</li><li>• Watch Officer</li><li>• Customer Service Specialist</li><li>• Systems Specialist</li></ul>

The FedTrak high-level architectural design schematic is presented in **Figure 3**.

The overall schematic is broken down into its component parts in **Figure 4**. The component decomposition presentation in Figure 4 is a "work in progress" document. The project team will use the component decomposition document as a working tool. It will be continuously expanded as the project team begins to develop working applications and as future project activities are completed.



**Figure 4. FedTrak System Schematic Decomposition Document**  
(Work in Progress)

FedTrak System Components	
Architectural Schematic Reference	Description/Purpose/Function
 <p><b>FedTrak<sup>1.</sup></b></p> <p>TSA Tier 1 Highway Security Sensitive Material Truck Tracking System</p> <p>The core components of the FedTrak system are:</p> <ul style="list-style-type: none"> <li>❖ Portals</li> <li>❖ Desktops</li> <li>❖ Databases</li> <li>❖ Applications</li> </ul>	<p><b>What is FedTrak?</b></p> <ul style="list-style-type: none"> <li>• An implementing tool for TSA's Tier 1 HSSM regulatory program.</li> <li>• A real-time tracking system for Tier 1 HSSM shipments that provides government security agencies with visibility into the movement of Tier 1 HSSMs, supports identification/management of the riskiest en-route shipments, and allows security agencies to predict and proactively manage security risks in advance of shipments.</li> <li>• A resource for government officials to support efficient and effective response operations by federal/state/local officials in the event of a problem with a Tier 1 HSSM shipment.</li> <li>• An on-line resource for Tier 1 HSSM shippers, carriers and consignees that have compliance responsibilities for their Tier 1 HSSM shipments.</li> <li>• An electronic manifest solution for Tier 1 HSSM shipments.</li> <li>• An electronic routing solution for Tier 1 HSSM shipments.</li> <li>• A valuable storehouse of data on Tier 1 HSSM shipments over U.S. roads.</li> </ul>
 <p><b>2. Shippers, Carriers and Consignees of Tier 1 Highway Security Sensitive Materials</b></p> <p>2. Tier 1 HSSM Shippers/Carriers</p> <p>Tier 1 HSSM Consignees 2.</p>	<p><b>What is a Tier 1 Highway Security Sensitive Material?</b></p> <p>TSA's highway security-sensitive security guidance recognizes two classes of highway security-sensitive materials:</p> <ul style="list-style-type: none"> <li>• <b>Tier 1 Highway Security-Sensitive Materials (Tier 1 HSSM)</b> – HSSM transported by motor vehicle whose potential consequences from an act of terrorism include a <b>highly significant</b> level of adverse effects on human life, environmental damage, transportation system disruption, or economic disruption.</li> <li>• <b>Tier 2 Highway Security-Sensitive Materials (Tier 2 HSSM)</b> - HSSM transported by motor vehicle whose potential consequences from an act of terrorism include <b>moderately significant</b> level of adverse effects on human life or health, environmental damage, transportation system disruption, or economic disruption.</li> </ul>

Data on Tier 1 HSSM shippers, carriers, and consignees is currently unavailable from TSA.

### How many Tier 1 HSSM shippers, carriers and consignees are there in the U.S.?

- **Tier 1 HSSM shippers = xx**
- **Tier 1 HSSM carriers = xx**
- **Tier 1 HSSM consignees = xx**
- **Number of Tier 1 HSSM shipments** – est. by TSA at about 2 million/year (see following figure)

### How many Tier 1 HSSM shipments are there in the U.S. each year?

- Tier 1 HSSM shipments = approx. **2 million** = 1,287,760 + Division 2.2 Tier 1 HSSM + Class 3 Flammable Liquids Tier 1 HSSM + Class B Corrosive Tier 1 HSSM

*TSA's Tier 1 HSSM List/Number of Shipments*




DOT Hazard Class	Hazmat Placard	Threshold Quantity	Number of Annual U.S. Shipments <sup>1</sup>
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	<del>Domestic - 563,771</del> <del>NAFTA - 6,767</del> <b>Tier 1 and Tier 2</b>
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

table continues next page

<sup>1</sup> 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.

The total number of annual Tier 1 HSSM shipments (1,287,760) in this figure does not include:






- Tier 1 HSSM Division 2.2 Non-Flammable Gas (also meeting the definition of a material poisonous by inhalation)

**OR**

- Tier 1 HSSM Class 3 Flammable Liquids (also meeting the definition of a material poisonous by inhalation)

**OR**

- Tier 1 HSSM Class 8 Corrosive Materials (also meeting the definition of a material poisonous by inhalation). Data is unavailable on the number of these shipments.

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	<del>Domestic - 62,015,889</del> <del>NAFTA - 119,816</del> <b>Tier 1 and Tier 2</b>
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	<del>Domestic - 4,548,595</del> <del>NAFTA - 95,703</del> <b>Tier 1 and Tier 2</b>
Other Materials		Any quantity of chemicals listed by the Chemical Weapons Convention on Schedules.	unknown
<b>Total</b>			<b>Domestic - 1,287.760+</b> <b>NAFTA - 34,235+</b> (see side note - total does not include Tier 1 Non-Flammable Gases, Tier 1 Class 3 Flammable Liquids or Tier 1 Class 8 Corrosives)

**Currently, TSA asks Tier 1/2 HSSM shippers, carriers, and consignees to voluntarily comply with TSA's HSSM Security Action Items.**

#### **TSA Security Action Items**

SAIs 1-16 apply to both Tier 1 and Tier 2 HSSMs.

SAIs 10-23 focus on en-route security of HSSM shipments.

SAIs 17-23 apply **only** to Tier 1 HSSMs.

#### **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

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

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

	<p><b>Security Action Item #11. Establish Appropriate Vehicle Security Program –</b> Employers should ensure that all company vehicles (power units including but not limited to tractors, straight trucks, pickups, and service units) are secured when unattended through use of primary and secondary securement systems.</p> <p>Primary methods should include the following:</p> <ul style="list-style-type: none"> <li>a) Ensuring that all company vehicles have the capability to be locked.</li> <li>b) Adopt a written security policy that includes: <ul style="list-style-type: none"> <li>i) procedures such as a key control program when a vehicle is not in active use, and</li> <li>ii) ensuring the vehicle engine is turned off, remove keys from vehicle, closing windows, and locking doors when the vehicle is in active use but unattended.</li> </ul> </li> </ul> <p>Secondary securement methods should include the following:</p> <ul style="list-style-type: none"> <li>a) Steering wheel locking system,</li> <li>b) Air brake locking system,</li> <li>c) Wheel locks, or</li> <li>d) Other appropriate lockout control process.</li> </ul> <p><b>Security Action Item #12. Establish Appropriate Cargo Security Program to Prevent Theft or Sabotage of Cargo Containers–</b> Employers should ensure that all cargo containers (including but not limited to trailers, tankers, straight trucks, security cages, and flatbeds) are secured when in use but unattended through use of a primary and secondary securement system. The primary methods should include the following: a) Ensuring that all cargo containers have the capability to be locked. b) Adopt a written security policy that includes: i) a key control program (if appropriate), and ii) ensuring a container is provided with a mechanical or electrical method of locking. Secondary securement method should include the following:</p> <ul style="list-style-type: none"> <li>a) Glad hand locks,</li> <li>b) King pin locks,</li> <li>c) Wheel locks, or</li> <li>d) Other appropriate lockout control process</li> </ul> <p><b>Security Action Item #13. Implement a Seal/Lock Control Program to Prevent Theft or Sabotage of Cargo –</b> Employers should implement a seal/lock program to prevent theft or sabotage of the contents of cargo containers and cylinders when in transport, when unattended by company personnel, or when at facilities incidental to transport. The following is recommended:</p> <ul style="list-style-type: none"> <li>Tier 1 HSSM – High security locks or electronic seals</li> <li>Tier 2 HSSM – Tamper evident (indicative) seals.</li> </ul> <p>When establishing a seal/lock control program employers should review the “ User’s Guide on Security Seals for Domestic Cargo” (January 2007) developed jointly by the Department of Homeland Security and Department of Defense.</p>
--	--

**Security Action Item #14. High Alert Level Protocols** – Employers should establish policies governing operations during periods of increased threat conditions under the Homeland Security Advisory System (for example when the DHS Threat Condition is raised from Orange to Red). These protocols should be capable of being implemented when deemed appropriate by an employer or appropriate law enforcement or homeland security officials. Alternatives to continued routine operations include:

- a) Identifying secure locations to seek refuge,
- b) For shipments exceeding 200 miles, identify private sector or law enforcement escorts to provide increased vehicle security, surveillance, and communications between local law enforcement officials and the motor vehicle while en route for shipments exceeding 200 miles or
- c) Other appropriate security measures identified by the employer.

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

**Security Action Item #15. Establish Security Inspection Policy and Procedures** – Employers should establish a security inspection policy and procedures for drivers to conduct security inspections. Security inspections should be performed in conjunction with required safety inspections conducted under 49 CFR Part 392 before operation of the vehicle. These security inspections should occur initially at the beginning of the driver's shift or trip (pre-departure) and after any stop en-route in which the vehicle is left unattended. The security inspection should consist of all areas where a suspicious item could be placed, training to recognize suspicious items, and reporting and response procedures to follow if a suspicious item or package is found.

**Security Action Item #16. Establish Reporting Policy and Procedures** – Employers should implement reporting procedures for drivers and non-driver employees to follow when reporting suspicious incidents, threats, or concerns regarding transportation facilities (terminal, distribution center, etc.) or company vehicles. These procedures should include at a minimum; appropriate company points of contact, appropriate law enforcement agencies, and the appropriate emergency response telephone number required in 49 CFR 172.604 and 172.606.

**Security Action Item #17. Shipment Pre-Planning, Advance Notice of Arrival and Receipt Confirmation Procedures with Receiving Facility** – The shipper (consignor), motor carrier and receiver (consignee) should conduct shipment pre-planning to ensure shipments are not released to the motor carrier until they can be transported to destination with the least public exposure and minimal delay in transit. Shipment pre-planning should include establishing the estimated time of arrival (ETA) agreeable to consignor, motor carrier, and consignee; load specifics (shipping paper information), and driver identification. When shipments are in transit, the motor carrier should coordinate with consignee to confirm the pre-established ETA will be met, or agree on a new ETA. Upon receipt of the shipment consignees should notify the shipper that the shipment has arrived on schedule and materials are accounted for. Methods for advance notice and confirmation of receipt of shipments include electronic mail and voice communications. When practical, consignees should immediately alert the appropriate shipper or motor carrier if the shipment fails to arrive on schedule or if a material shortage is discovered. Methods for immediate alert notifications should be made by voice communications only. Where immediate notification is not practical (for example at unmanned facilities), the consignor, the motor carrier, and consignee should agree on alternate confirmation (method and time) of delivery and receipt. Consignees should make every effort possible to accept a shipment that arrives during non-business hours due to unforeseen circumstances.

**Security Action Item #18. Preplanning Routes** – Employers should ensure preplanning of primary and alternate routes. This preplanning should seek to avoid or minimize proximity to highly populated urban areas or critical infrastructure such as bridges, dams, and tunnels. Policies governing operations during periods of Orange or Red alert levels under the Homeland Security Advisory System should plan for alternate routing for TIER 1 HSSM shipments away from highly populated urban areas and critical infrastructure. The motor carrier or law enforcement officials may determine when to implement alternate routing. Drivers should be encouraged to notify the company’s dispatch center when substantial en-route deviation is necessary.

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

**Security Action Item #20. Dedicated Truck** – Employers should implement policies to ensure that, except under emergency circumstances, contracted shipments remain with the primary carrier and are not subcontracted, driver/team substitutions are not made, and transloading does not occur unless the subcontractor has been confirmed to comply with applicable Federal safety and security guidance and regulations and company security policies.

**Security Action Item #21. Tractor Activation Capability** – Employers should implement security measures that require driver identification by login and password or biometric data to drive the tractor. Companies should provide written policies and instructions to drivers explaining the activation process.

**Security Action Item #22. Panic Button Capability** – Employers should implement means for a driver to transmit an emergency alert notification to dispatch. “Panic Button” technology enables a driver to remotely send an emergency alert notification message either via Satellite or Terrestrial Communications, and/or utilize the remote Panic Button to disable the vehicle.

**Security Action Item #23. Tractor and Trailer Tracking Systems** – Employers should have the ability of implementing methods of tracking the tractor and trailer throughout the intended route with satellite and/or land-based wireless GPS communications systems. Tracking methods for the tractor and trailer should provide current position by latitude and longitude. Geo-fencing and route monitoring capabilities allow authorized users to define and monitor routes and risk areas. If the tractor and/or trailer deviates from a specified route or enters a risk area, an alert notification should be sent to the dispatch center. An employer or an authorized representative should have the ability to remotely monitor trailer “connect” and “disconnect” events. Employers or an authorized representative should have the ability to poll the tractor and trailer tracking units to request a current location and status report. Tractor position reporting frequency should be configured at not more than 15-minute intervals. Trailer position reporting frequency should be configured to provide a position report periodically when the trailer has been subject to an unauthorized disconnect from the tractor. The reporting frequency should be at an interval that assists the employer in locating and recovering the trailer in a timely manner. The tractor and trailer tracking system should be tested periodically and the results of the test should be recorded

TSA Tier 1 HSSM regulations will be based on Security Action Items, and will establish requirements for shippers, carriers, and fleet tracking vendors.

**TSA plans to implement a regulatory program for Tier 1 HSSM shipments based on the Security Action Items. What elements will TSA likely include in its Tier 1 HSSM regulatory program?**

Potential Tier 1 HSSM Regulatory Elements		
Tier 1 HSSM Shippers	Tier 1 HSSM Carriers	Fleet Tracking Vendors
<ul style="list-style-type: none"> <li>• Register with TSA Tier 1 HSSM truck tracking center.</li> <li>• File electronic manifest with TSA Tier 1 HSSM truck tracking center before "gate out".**</li> <li>• File electronic route plan with TSA Tier 1 HSSM truck tracking center before "gate out". **</li> <li>• May not release a Tier 1 HSSM shipment to a driver that does not have a CDL with a hazmat extension or to a carrier that does not possess a hazmat safety permit.</li> </ul> <p>** Requirement may also be satisfied by shipper's carrier</p>	<ul style="list-style-type: none"> <li>• Deploy compliant smart truck devices and use compliant Fleet Tracking Vendor.</li> <li>• Register with the TSA Tier 1 HSSM truck tracking center.</li> <li>• Use the services of a truck tracking vendor that has TSA Tier 1 HSSM truck tracking center compliant systems and service offerings.</li> <li>• Respond to inquiries and alerts issued by the TSA Tier 1 HSSM truck tracking center.</li> <li>• Must have the ability to communicate with a driver hauling a Tier 1 HSSM shipment.</li> <li>• Provide drivers of Tier 1 HSSM shipments the ability to send a panic alert.</li> </ul>	<ul style="list-style-type: none"> <li>• Report the location of a carrier's vehicle hauling a Tier 1 HSSM shipment to the TSA Tier 1 HSSM truck tracking center in a manner and at a polling frequency specified by the Transportation Security Center.</li> <li>• Report alerts and messages from installed smart truck devices on the carrier's vehicle to the TSA Tier 1 HSSM truck tracking center in a manner and frequency specified by the TSA Tier 1 HSSM truck tracking center.</li> <li>• Respond to the TSA Tier 1 HSSM truck tracking center system messaging: location reporting and vehicle immobilization (system to system 2-way communications).</li> </ul>

FedTrak must meet a number of functional requirements to support TSA's Tier 1 HSSM regulatory program.

**What functional requirements should a Tier 1 HSSM truck tracking system meet to support a regulatory program based on SAIs?**

Implication of SAI 17 – SAI 23 for Tier 1 HSSM Shipments	
Tier 1 HSSM Carrier Technology Deployment	
Core Technology	Truck-mounted GPS Receiver On-board Computer Wireless Modem WiFi-Enabled Smart Phone
Additional Devices	Untethered Trailer Tracking System Driver authentication & Vehicle Immobilization System In cab &/or Remote Driver Panic Buttons
Functional Requirements Tier 1 HSSM Truck Tracking System	
<ul style="list-style-type: none"> <li>✓ Users must be able to enter an electronic manifest (load type/quantity; shipper, carrier and receiver information; driver information; vehicle information; estimated time of arrival).</li> <li>✓ Users must be able to enter primary and alternate routes (electronic route plan).</li> <li>✓ System should automatically monitor route adherence and send alerts as needed. Also, monitor location shipment location in relation to critical infrastructure. Dynamic risk profiling of shipments.</li> <li>✓ System should process alerts (panic button, untethered trailer tracking, vehicle immobilization) from truck tracking vendors.</li> <li>✓ System must be able to accept "gate out" and "gate in" notifications.</li> </ul>	

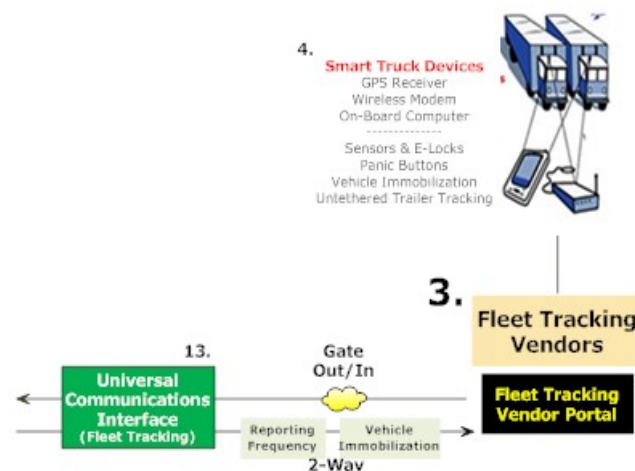
		<ul style="list-style-type: none"> <li>✓ System should monitor shipment chain-of-custody between “gate out” and “gate in”.</li> <li>✓ The business processes underlying the TSA Tier 1 HSSM requirements should be automated with monitoring systems serving as the messaging mechanism.</li> <li>✓ System should be able to alert en-route carriers/drivers that Orange or Red conditions have been implemented by DHS and that alternate routing should be taken.</li> <li>✓ System should be able to accept carrier input that the driver is delayed (ETA change) or that the driver is taking an alternate route.</li> </ul>	
--	--	--	--

### 3. Fleet Tracking Vendors

#### Regulations

Tier 1 HSSM fleet tracking vendors must report data from Tier 1 HSSM trucks to TSA’s truck tracking center using the published Universal Communications Interface.

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



The cost of deploying and operating “smart truck” technology systems is low and the market for smart truck technology is well established (see SERRI Section 3.1.2). Hazmat carriers use the services of commercial fleet tracking vendors such as Qualcomm and Safefreight Technology (see SERRI Figure 3.1.b).

TSA and FedTrak will leverage the technology offered by existing commercial fleet tracking vendors. The FMCSA study (see SERRI Section 4.1) and the TSA Hazmat Truck Security Pilot program (see SERRI Section 4.5) demonstrated the value of leveraging the product/service offerings of commercial fleet tracking vendors. Fleet tracking vendors have the ability to forward on vehicle location and other alerts to a hazmat truck tracking center using a real-time XML data feed.

Commercial fleet tracking vendors anticipate that government regulation will dictate the deployment of “smart truck” technology for certain types of hazmat shipments (see SERRI Section 5.1). Product development by “smart truck” technology vendors has increasingly focused on developing product security features, and product marketing has increasingly emphasized hazmat shipment security. Fleet tracking vendors may need to fine-tune their “smart truck” product offerings to meet TSA’s Tier 1 HSSM requirements and FedTrak’s need for a complete set of data that it needs to operate a fully functioning truck tracking system (see SERRI Section 6.4.1.7). However, these modifications will be relatively minor. Refer to Appendix A of the SERRI Analysis Update (Deliverable 1.1)

#### 4. Smart Truck Devices

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



Section 2 (pages 5-8) of the SERRI Analysis Update (Deliverable 1.1) describes how “smart truck” technology works.

The cost of deploying and operating “smart truck” technology systems is low and the market for smart truck technology is well established (see SERRRI Section 3.1.2). Hazmat carriers use the services of commercial fleet tracking vendors such as Qualcomm, PeopleNet, and Safefreight Technology.

Section 3 (pages 8-22) of the SERRI Analysis Update (Deliverable 1.1) describes some of the commercial “smart truck” systems offered by fleet tracking vendors. Appendix A of the SERRI

Analysis Update (Deliverable 1.1) is particularly insightful as it contains technical literature and product information on the “smart truck” systems offered by Qualcomm, PeopleNet, and Safefreight Technology.

FedTrak will leverage the technology offered by existing commercial fleet tracking vendors. The FMCSA study (see SERRI Section 4.1) and the TSA Hazmat Truck Security Pilot program (see SERRI Section 4.5) demonstrated the value of leveraging the product/service offerings of commercial fleet tracking vendors. Fleet tracking vendors have the ability to forward on vehicle location and other alerts to a hazmat truck tracking center using a real-time XML data feed.

Commercial fleet tracking vendors anticipate that government regulation will dictate the deployment of “smart truck” technology in segments of the hazmat transportation market (see SERRI Section 5.1). Product development by “smart truck” technology vendors has increasingly focused on developing product security features, and product marketing has increasingly emphasized hazmat shipment security. Refer to Appendix A of the SERRI Analysis Update (Deliverable 1.1).

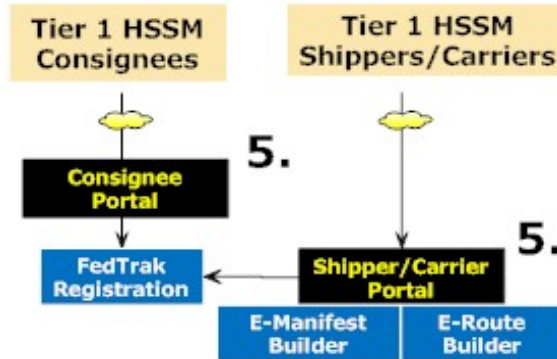
## 5. Shipper, Carrier, & Consignee Portals

(Registration, E-Manifest, E-Route)

**A FedTrak portal will be the doorway that Tier 1 shippers, carriers, and consignees will use to access FedTrak applications/data.**

A **web portal** presents information from diverse sources in a unified way. Portals provide a way for enterprises to provide a consistent look and feel with access control and procedures for multiple applications. (Wikipedia)

Portal sites connect people to business-critical information, expertise, and applications. The project team will use the Microsoft Office SharePoint Server as its enterprise portal platform. Using SharePoint will make it easy to build and maintain FedTrak portals.



Tier 1 HSSM shippers, carriers, and consignees will interact with FedTrak via portals. They will have 24/7 access to corporate data through a portal, and will be able to edit corporate information online. For example, a carrier can add or delete drivers or customers. Shippers, carriers, and consignees will also have access to shipment data (in transit and completed) via a portal.

Note that every user rights will be assigned to individuals in FedTrak. Each person registered in FedTrak by a shipper, carrier, or consignee will have their own portal.

The project team will build portal interfaces for Tier 1 HSSM shippers, carriers and receivers. As indicated in the figure below, the structure and content of these portals will be determined in a later stage of the project.

Information/Applications Available Via FedTrak Portals			
	Shipper	Carrier	Consignee
Applications Via Portal	<ul style="list-style-type: none"> <li>Electronic manifest</li> <li>Electronic route plan</li> <li>Edit corporate information &amp; user rights</li> </ul>	<ul style="list-style-type: none"> <li>Electronic manifest</li> <li>Electronic route plan</li> <li>Edit corporate information &amp; user rights</li> </ul>	<ul style="list-style-type: none"> <li>Edit corporate information &amp; user rights</li> </ul>
Information Via Portal/Portal Look and Feel	<ul style="list-style-type: none"> <li>tbd</li> </ul>	<ul style="list-style-type: none"> <li>tbd</li> </ul>	<ul style="list-style-type: none"> <li>tbd</li> </ul>

## 6. FedTrak Registration

### Regulations

Tier 1 HSSM shippers, carriers, and consignees must register with TSA's truck tracking center.

### Intake

- Shippers, carriers, and consignees will have different user interfaces for registration (ie carriers need to provide FedTrak different information than shippers).
- Registration interfaces will be built using Infopath/Biztalk.
- FedTrak will use ACE Truck E-Manifest data conventions for:
  - Drivers
  - Conveyances (power units)
  - Equipment (trailers, containers, etc.)
  - Shipper
  - Consignee
- Tier 1 HSSM trading partners (shippers, carriers, and consignees) will establish corporate affiliations during registration.

### Analysis

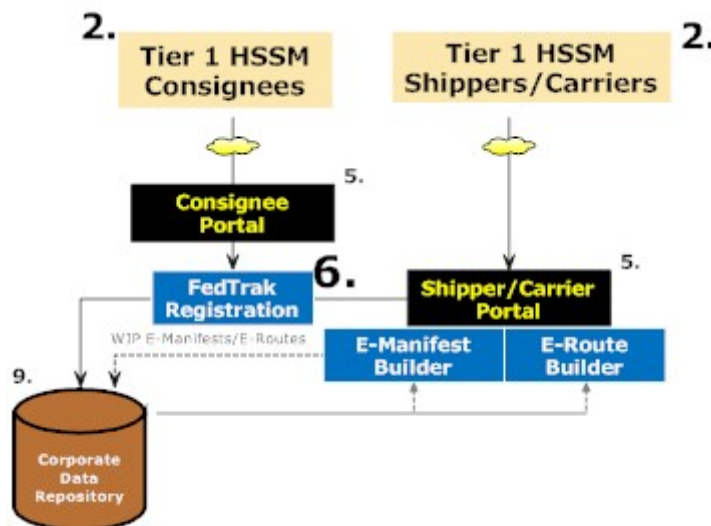
- N.A.

### Dissemination

- Corporate information collected during registration will be fed into the FedTrak Corporate Data Repository.

**FedTrak Registration is an application for Tier 1 shippers, carriers and consignee. ....**

A truck tracking center needs access to corporate data from Tier 1 HSSM shippers, carriers and consignees to feed manifest and routing applications. A registration process is the most efficient means to gather and organize this data for use in FedTrak applications. Otherwise, basic corporate data will have to be entered every time a manifest or routing application is used.



TSA regulations will require Tier 1 HSSM shippers, carriers and consignees to complete registration. The FedTrak registration application will be built using Infopath/Biztalk.

FedTrak will use the Standard Carrier Alpha Code as the key identifier for Tier 1 HSSM carriers. Serial numbers on fleet tracking equipment will be captured during registration.

FedTrak will use ACE Truck E-Manifest data conventions to support the FedTrak registration application:

- Drivers
- Conveyances (power units)
- Equipment (trailers, containers, etc.)
- Shipper
- Consignee

Tier 1 HSSM trading partners will establish corporate affiliations during registration. See Section 1.2 for a chart illustrating expectations for establishment of corporate affiliations in FedTrak.

Tier 1 HSSM trading partners will establish user rights during registration. See Section 1.2 for a chart illustrating expectations for establishment of user rights in FedTrak.

## 7. E-Manifest Builder

### Intake

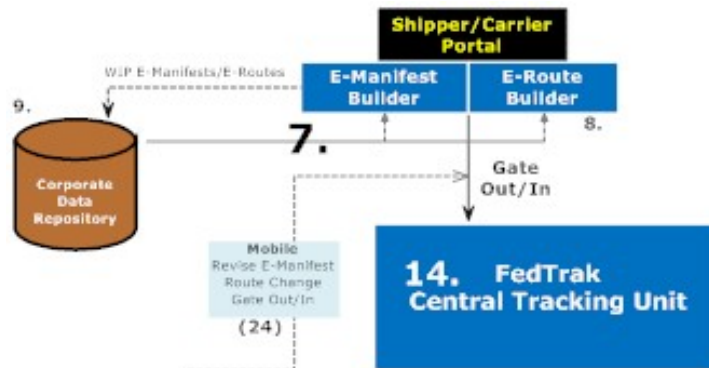
- E-Manifest Builder application accessible via a shipper or carrier portal
- FedTrak presents shipper/consignee information from the Corporate Data Repository in pick list format (shipper-consignee paired data)
- FedTrak presents shipper/consignee information in pick list format
- Carrier information from the Corporate Data Repository (pre-filled on electronic manifest form)
- FedTrak presents driver, equipment, conveyance information from Corporate Data Repository in pick list format
- FedTrak presents HSSM information from Corporate Data Repository (template or pick list format); carrier adds quantity information for each HSSM type
- FedTrak will accept electronic manifest uploads from corporate ERP systems

### Analysis

- FedTrak uses Infopath/Biztalk to combine data into a complete electronic manifest ready for carrier digital signature; FedTrak performs data validation and error checking
- FedTrak checks user rights to prevent

**E-manifest Builder is an application that Tier 1 HSSM shippers and receivers will use to build and file a FedTrak electronic manifest.**

FedTrak will use an electronic manifest application to monitor Tier 1 HSSM shipment chain of custody.



FedTrak's registration and electronic manifest applications will incorporate data standards developed for the Customs & Border Protection's ACE Truck E-Manifest system. The ACE truck e-manifest program has developed five master sets of data elements that will support e-manifest preparation.

- Drivers
- Conveyances (power units)
- Equipment (trailers, containers, etc.)
- Shipper
- Consignee

Building an electronic manifest will be quick and easy – pick lists drawn from the Corporate Data repository will speed manifest preparation. Section 1.2 describes pick list categories and the pick list process for building an electronic manifest.

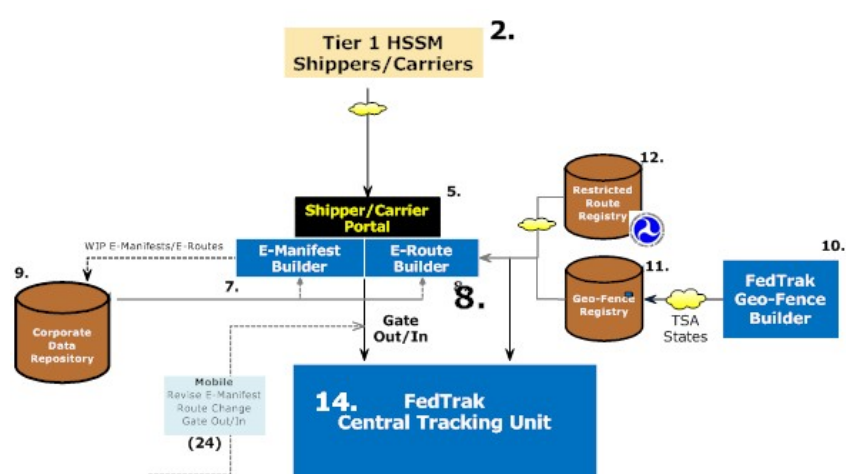
E-manifests will draw from corporate registration data in FedTrak.com™. For example, when a shipper prepares an e-manifest, the on-line form will be pre-populated with the shipper's corporate data (shipping location, material type, etc.) collected earlier when the shipper completed registration in FedTrak.com™.

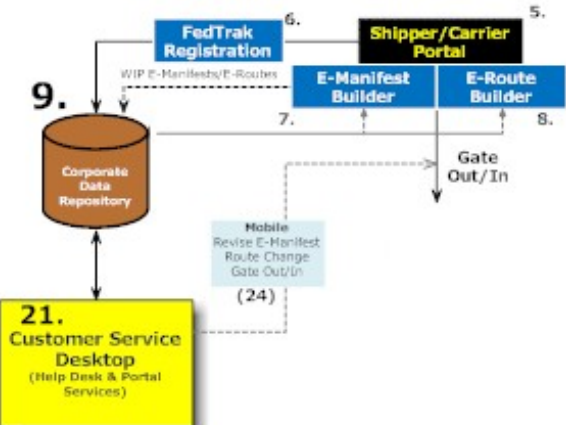
FedTrak will use Microsoft's electronic form tool, Infopath, to build its electronic manifest application. Refer to SERRI report for a description of XFML form technology. Tier 1 HSSM shippers/carriers will prepare and file electronic manifests via the FedTrak portal.

The FedTrak electronic manifests will use digital signatures to promote document security and to support chain of custody monitoring. An electronic manifest has to be signed prior to "gate out" in order for FedTrak to gain visibility for that shipment.

Most Tier 1 HSSM shipments will have only one Tier 1 HSSM on the truck and a single manifest for the shipment (one shipper, one manifest, one consignee). However, shipments from a single shipper may have multiple manifests and multiple consignees (one shipper, multiple manifests, multiple consignees).

E-manifest transactions – such as application of digital signatures – are transactions that FedTrak will receive and

<p>unauthorized persons from completing a manifest transaction</p> <ul style="list-style-type: none"> <li>FedTrak electronic manifest application supports partial form signatures; partial form locking</li> <li>FedTrak logs electronic manifest transactions as they occur</li> </ul> <p><b>Dissemination</b></p> <ul style="list-style-type: none"> <li>Draft manifest stored in Corporate Data Repository; ready for inclusion in the carrier's FedTrak Trip Plan</li> <li>Signed manifest stored in Corporate Data Repository</li> <li>Manifest transactions stored in Corporate Data Repository</li> </ul>	<p>process. A carrier's digital signature on an electronic manifest, for example, signals FedTrak that a new Tier 1 HSSM shipment is being initiated.</p>
<p><b>8. E-Route Builder</b></p> <p><b>Intake</b></p> <ul style="list-style-type: none"> <li>WIP – later tasks will define</li> </ul> <p><b>Analysis</b></p> <ul style="list-style-type: none"> <li>WIP – later tasks will define</li> </ul> <p><b>Dissemination</b></p> <ul style="list-style-type: none"> <li>WIP – later tasks will define</li> </ul>	<p><b>E-Route Builder is an application that Tier 1 HSSM Carriers will use to build electronic route plans.</b></p> <p>Electronic route plans are critical to a truck tracking program. Without an electronic route plan, a truck tracking system cannot track carrier route adherence. As a result, geo-fence and risk management capabilities of a truck tracking system would be substantially degraded.</p> <p>Like the electronic manifest, the electronic route plan must be submitted as part of a FedTrak Trip Plan prior to "gate out" so that the truck tracking center can match the vehicle's location with its planned route</p> <p>PL 110-53 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</p>  <pre> graph TD     2[Tier 1 HSSM Shippers/Carriers] --&gt; 5[Shipper/Carrier Portal]     5 --&gt; 7[E-Manifest Builder]     5 --&gt; 8[E-Route Builder]     9[(9. Corporate Data Repository)] -- "WIP E-Manifests/E-Routes" --&gt; 7     7 --&gt; 14[14. FedTrak Central Tracking Unit]     8 --&gt; 14     14 -- "Gate Out/In" --&gt; 8     14 -- "Mobile Revise E-Manifest Route Change Gate Out/In (24)" --&gt; 7     12[(12. Restricted Route Registry)] --&gt; 8     11[(11. Geo-Fence Registry)] --&gt; 8     10[10. FedTrak Geo-Fence Builder] -- "TSA States" --&gt; 11   </pre>

	<p>written or electronic format. FedTrak.com™ will allow carriers to prepare and submit electronic route plans on-line that meet PL 110-53 requirements. Carriers will be required to select an electronic route plan in FedTrak™ before “gate out” of a Tier 1 HSSM shipment. After “gate out”, FedTrak™ systems will track the movement of Tier 1 HSSM shipments against the electronic route plan filed by the carrier.</p> <p>Tier 1 HSSM shippers/carriers will use the FedTrak route-authoring tools to prepare electronic route plans. A shipper or carrier will be able to prepare and store multiple routes on FedTrak.</p> <p>Refer to Section 1.2 for more detail on electronic route plan preparation in FedTrak.</p>
<p><b>9. Corporate Data Repository</b></p> <p><b>Intake</b></p> <ul style="list-style-type: none"> <li>• Corporate data from registration (shippers, carriers, consignees)</li> <li>• Draft electronic manifests</li> <li>• Draft electronic route plans</li> <li>• Draft trip plan</li> <li>• Customer service records</li> <li>• En-route shipment transaction data</li> <li>• Completed shipment transaction data</li> </ul> <p><b>Analysis</b></p> <ul style="list-style-type: none"> <li>• N.A,</li> </ul> <p><b>Dissemination</b></p> <ul style="list-style-type: none"> <li>•</li> </ul>	 <p>Additional details after database design task.</p>
<p><b>14. Central Tracking Unit</b></p>	<p>The Central Tracking Unit (CTU) of FedTrak.com™ will efficiently merge data to create actionable information. As illustrated in Figure 1 in Section 1.1, the following questions about an individual shipment can be answered once the data is merged.</p>

### Intake

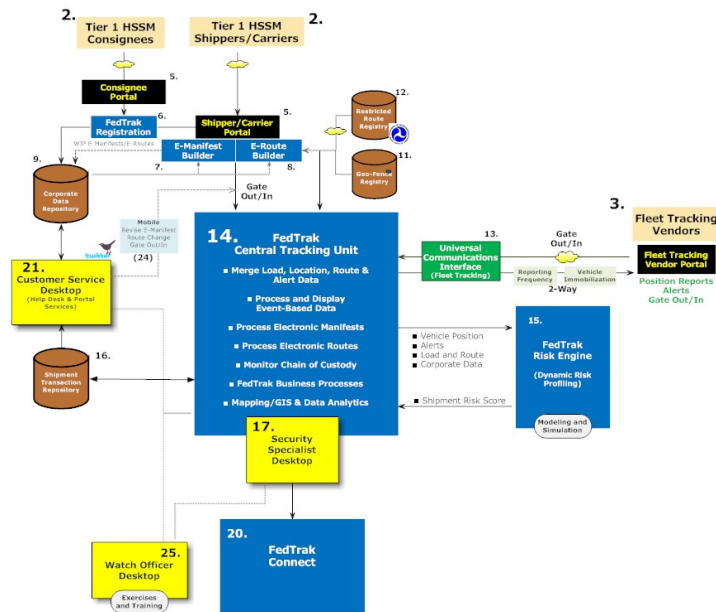
- Alerts and location from Fleet Tracking Vendor systems via the UCI
- Restricted routes for hazmat shipments from DOT Restricted Route Registry database (external to FedTrak) – note geospatial data component.
- Geo-fences constructed by TSA and state agencies from FedTrak Geo-Fence Registry database (internal to FedTrak) – note geospatial data component.
- Load – electronic manifest prepared by shipper or carrier using FedTrak E-Manifest Builder. Shipper/carriers will access E-Manifest Builder via MyFedTrak Portal.
- Route – electronic route plan prepared by shipper or carrier using FedTrak E-Route Builder. Shipper/carriers will access E-Route Builder via MyFedTrak Portal – note geospatial data components.
- Shipment risk scores from the FedTrak Risk Engine.

### Analysis

- WIP – later tasks will define

### Dissemination

- WIP – later tasks will define



- 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?

Additional detail after database design task

## 15. FedTrak Risk Engine

### Intake

- Shipment load information – type and quantity of Tier 1 HSSMs
- Shipper information
- Carrier information
- Consignee information
- Driver information
- Route plan
  - origination point of shipment
  - expected routing
  - end point (consignee location)
- Past transactions and events
- Alerts from fleet tracking vendor
- Location updates from fleet tracking vendor
- Intelligence updates from FedTrak Intelligence Specialist

### Analysis

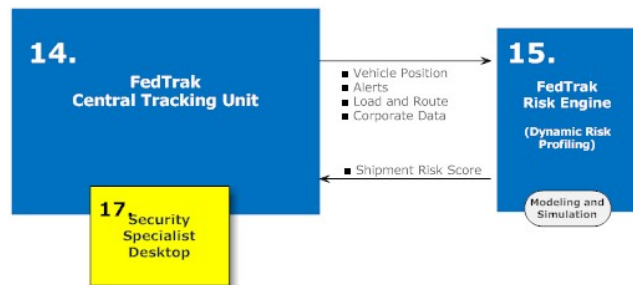
- Business rules for calculating shipment risk score TBD

### Dissemination

- Risk score published back to Central Tracking Unit
- Score recalculated every time any data – such as vehicle location – changes; score republished back to CTU

The FedTrak risk engine will assign risk scores to Tier 1 HSSM shipments. A COTS business rules engine will be incorporated into the FedTrak system.

TSA's Hazmat Truck Security Pilot prototype was limited in functionality and tracked only a small number of hazmat shipments. FedTrak.com™ will be designed to track 2+ million hazmat shipments per year. To be viable under this transaction loading, FedTrak must identify the "riskiest" shipments and present information on them to FedTrak Security Specialists so that they can efficiently manage "real" emerging threats. Too many "false positives" will create an overwhelming workload that will prevent Security Specialists from effectively managing their oversight responsibilities.



The Central Tracking Unit will feed data on Tier 1 HSSM shipments to the risk engine. The risk engine will be built using a COTS business rules engine. Section 3.8 of the SERRI report describes how business rules engines work, and how they may be integrated into an application like FedTrak. A number of commercial business rule products are available.

As illustrated in the figure, the CTU will feed data to the risk engine. The risk engine will process the data using programmed business rules and pass risk scores back to CTU.

FedTrak's risk engine will calculate an initial risk score for a shipment when the carrier files a final trip plan for the shipment. At that point, the type/quantity of HSSMs is known and the route the driver will follow is known. Also, information on the shipper and consignee – including information on past shipments between them – can be factored into the scoring. The first update to the shipment risk score will be at "gate out".

The risk score for a Tier 1 HSSM shipment will change as the vehicle travels from "gate out" to "gate in". For example, every 15 seconds CTU will post new vehicle location data for the shipment, and the risk engine will recalculate the risk score for the shipment. If the shipment is nearing a geographic area protected by a geo-fence, for example, the risk score of the shipment will rise. Other alerts or messages (driver panic button, off-route shipment, unexpected offloading, etc.) will also be sent to the risk engine from CTU. Each alert or message will cause the risk engine to recalculate the shipment's risk score.

The risk engine will continually update the risk scores of Tier 1 HSSM shipments. A high risk score will put a shipment on top of the list of shipments that FedTrak Security Specialists will actively monitor. A driver panic alert, for example, will immediately push a shipment risk score up to a very high score prompting direct intervention by a Security Specialist.

	<p>False positives are a significant issue in setting business rules to support Tier 1 HSSM shipment tracking. Identifying too many shipments as shipments of concern will unnecessarily require overstaffing at the FedTrak operations center and cause Security Specialists to contact TSA and State action agencies too frequently. Identifying too few shipments as shipments of concern invites a missed opportunity to prevent a terrorist act</p> <p>THE RISK ENGINE will also calculate the population at risk from each Tier 1 HSSM shipment. This calculation will be dynamic – it will change frequently as the truck’s location changes – and will be based on the characteristics of the HSSMs on board the truck and the population near the shipment at any time.</p> <p>Population at risk calculations will be aggregated to present the population at risk on a state-by-state basis as well as the overall national population at risk.</p>
<b>16. Shipment Transaction Repository</b>	Additional detail with completion of database design task
<b>17. Security Specialist Desktop</b>	WIP – later tasks will define
<b>18. FedTrak Operations Repository</b>	Additional detail with completion of database design task
<b>19. Intelligence Analyst Desktop</b>	WIP – later tasks will define
<b>20. FedTrak Connect</b>	WIP – later tasks will define
<b>21. Customer Service Desktop</b>	WIP – later tasks will define
<b>22. Government Portal</b>	WIP – later tasks will define
<b>23. Shipper/Carrier Portal</b>	See #5
<b>24. FedTrak Mobile Applications</b>	WIP – later tasks will define
<b>25. Watch Officer Desktop</b>	WIP – later tasks will define
<b>26. System Security Desktop</b>	WIP – later tasks will define
<b>27. TSA HQ Portal</b>	WIP – later tasks will define

## 4.0 FedTrak Operational Scenarios

Section 2 described the FedTrak architectural schematic developed by the project team. The project team examined two operational scenarios as an exercise to articulate the functionality the project team intends to include in the FedTrak system.

1. Preparation of a trip plan for a Tier 1 HSSM shipment (carrier)
2. Tier 1 HSSM shipment from gate out to gate in – no en-route shipment problems
3. Risk score spike for en-route Tier 1 HSSM shipment (driver panic button)

Scenario 1 discussions – preparation of a trip plan for a Tier 1 HSSM shipment - are summarized in Section 1.2. Scenarios 2 and 3 are summarized in Section 4.1 and 4.2.

The project team also constructed a number of additional scenarios that FedTrak may be called on to support. The project team will develop these scenarios into test cases for system validation in later phases of the project.

Additional FedTrak Operational Scenarios	
Preparation of a trip plan for a Tier 1 HSSM shipment (carrier)	Describes how a Tier 1 HSSM carrier will prepare manifests and a route plan and merge them into a trip plan for a shipment. Refer to Section 1.2 for detailed mechanics.
Amendment of draft electronic manifest by carrier at shipper facility	Describes how a driver would use the FedTrak mobile application to modify a draft electronic manifest in the FedTrak system. Driver will change the quantity of materials in the shipment. Driver will apply a digital signature to the electronic manifest.
Amendment to route plan by carrier – en-route shipment	Describes how a carrier will file an amended trip plan for a Tier 1 HSSM shipment while the shipment is en-route.
TSA declares Transportation Security Incident (hijacking with terrorist intent)	Describes how FedTrak will work when TSA declares a Transportation Security Incident. Scenario involves hi-jacking of an en-route Tier 1 HSSM shipment.
CNN and the missing Tier 1 HSSM shipment (Ed Bowers needs to know right now)	Describes a scenario in which CNN reports that a high hazard material (phosgene) has been found in Manhattan. DHS officials turn to TSA executives to account for all shipments of phosgene. Ed Bowers, TSA executive, contacts FedTrak Watch Officer with urgent request for information and analysis.
DHS declares RED threat level	Describes a scenario in which DHS declares Red threat level and directs Tier 1 HSSM carriers to find safe harbors for en-route shipments. Describes how FedTrak might

	support Tier 1 carriers as they react to the declaration by DHS.
Tier 1 HSSM shipments and the VIP's schedule	A VIP is scheduled to be at a certain place at a certain time. Describes how FedTrak will support security personnel interested in making sure that the VIP and scheduled Tier 1 HSSM shipments do not cross paths. Also, describes how security personnel can draw upon FedTrak to monitor movements of Tier 1 HSSMs in and around a VIP on a real-time basis.
Tier 1 HSSM shipments and LEPC officials	Local emergency planning committees are responsible for preparing contingency plans for hazmat incidents. This scenario involves a planning/field exercise by a major metropolitan planning agency. It describes how FedTrak will help LEPCs prepare better plans, and how FedTrak will support a field exercise (spill, hijacking, etc.).
Tier 1 HSSM shipments and the state vehicle enforcement officer	Describes how FedTrak mobile applications will support a state vehicle enforcement officer at a roadside weigh station or during a routine traffic stop/inspection of a Tier 1 HSSM shipment.
Detection of anomalies in Tier 1 HSSM shipments (FedTrak Intelligence Analyst)	Describes how a FedTrak Intelligence Analyst will use business analytics/GIS tools to detect anomalies in Tier 1 HSSM shipment patterns that indicate the possibility of a terrorist threat.
Tier 1 HSSM shipment – accident/spill on an Interstate road passing through a metropolitan area.	Describes how FedTrak will support state action agencies, municipal/county agencies, and first responders in the event of an accident/spill of a Tier 1 HSSM shipment.

<b>Scenario Name</b>	<b>4.1 Tier 1 HSSM shipment from gate out to gate in – no en-route shipment problems</b>
<b>Primary Actor</b>	Tier 1 HSSM Carrier/Driver
<b>Secondary Actor(s)</b>	Tier 1 HSSM Shipper Tier 1 HSSM Consignee
<b>Brief Description</b>	<p>This scenario involves a Tier 1 HSSM shipment that travels from “gate out” to “gate in” without incident.</p> <p>The shipment risk score never rises high enough to warrant close scrutiny by FedTrak Security Specialists. The carrier will drop part of the load with Consignee 1 before leaving the remainder of the load with Consignee 2. Also, the carrier will stop at a safe harbor location to rest during the trip.</p> <p>After dropping part of the load with Consignee 1, the driver will travel through an urban area. The shipment risk score will rise but never high enough to cause undue concern by FedTrak Security Specialists.</p>
<b>Precondition</b>	<p>Registration by shipper/carrier/consignee</p> <p>Preparation of e-manifest by carrier</p> <p>Preparation of e-route plan by carrier</p> <p>Preparation of trip plan by carrier</p>
<b>Trigger(s)</b>	<p>Application of digital signature on e-manifest by driver signifying shipment custody exchange from shipper to carrier</p> <p>Gate out signal by driver (indicating shipment is en-route)</p>
<b>Flow of Events</b>	<p>Gate out to gate in workflow</p> <ul style="list-style-type: none"> <li>• Driver manifest digital signature; assumption of shipment custody</li> <li>• Gate out at shipper’s facility</li> <li>• Initial shipment risk score by FedTrak risk engine</li> <li>• Location reporting and risk score updates to CTU via fleet tracking vendor</li> <li>• Gate in signal by driver – consignee 1 (via FedTrak Mobile)</li> <li>• Consignee digital signature for manifest(s) for portion of load intended for consignee 1 (via FedTrak Mobile)</li> <li>• Manifest signature/assumption of shipment custody – consignee 1</li> <li>• Gate out signal by driver – consignee 1 (via FedTrak Mobile)</li> <li>• Pass through urban area (elevated risk score)</li> <li>• Safe harbor gate in signal by driver (via FedTrak Mobile)</li> <li>• Safe harbor gate out by driver (via FedTrak Mobile)</li> </ul>

	<ul style="list-style-type: none"> <li>• Gate in – consignee 2</li> <li>• Manifest signature and assumption of shipment custody</li> </ul>
<b>Post conditions</b>	Detailed shipment transaction details are stored in the Shipment Transaction Repository. Shippers, carriers, and consignees are able to view data on the en-route shipment via their portals. Shippers, carriers, and consignees are able to retrieve data on the transaction after it is completed via their portals.
<b>Alternate Flows and Exceptions – other scenarios</b>	Not applicable.
<b>FedTrak Components</b>	Business Rules Engine Central Tracking Unit Shipment Transaction Repository Security Specialist Desktop Universal Communications Interface FedTrak Mobile
<b>Assumptions</b>	None
<b>Issues</b>	<ul style="list-style-type: none"> <li>• Is safe harbor location information available? In what format?</li> </ul>

<b>Scenario Name</b>	<b>4.2 Risk score spike for en-route Tier 1 HSSM shipment (driver panic button)</b>
<b>Primary Actor</b>	FedTrak Security Specialist
<b>Secondary Actor(s)</b>	Tier 1 HSSM Carrier Tier 1 HSSM Driver
<b>Brief Description</b>	This scenario involves an en-route Tier 1 HSSM shipment. A driver panic button alert is received by FedTrak, prompting an instantaneous risk score spike that places the shipment at the top of a Security Specialist's list for action.
<b>Precondition</b>	<ul style="list-style-type: none"> <li>• Pre-shipment activities <ul style="list-style-type: none"> <li>○ Carrier prepares e-manifest</li> <li>○ Carrier prepares e-route plan</li> <li>○ Carrier files trip plan</li> <li>○ Driver digital signature on manifest</li> </ul> </li> <li>• Gate out</li> </ul>
<b>Trigger(s)</b>	<p>Panic button alert from Tier 1 HSSM driver while shipment is between Gate Out and Gate In.</p> <p>Note: the driver panic button alert is one of many things that might trigger a shipment risk score spike. Other possible causes of an en-route risk score spike include the following.</p> <ul style="list-style-type: none"> <li>• Driver panic button (in cab – dashboard panic button)</li> <li>• Driver alert (out of cab – keyfob panic button)</li> <li>• Driver initiated suspicious activity report</li> <li>• Hijacking attempt</li> <li>• Unexpected loss of signal – truck out of contact too long</li> <li>• Unauthorized driver attempts to take custody of a shipment</li> <li>• Off route shipment (significant deviation; no route change notice filed)</li> <li>• TSA security bulletin (regional and/or generic material type)</li> <li>• Unexpected trailer separation</li> <li>• Equipment tampering</li> <li>• Suspicious activity report (individual truck/shipment)</li> <li>• Gate out message but no manifest/route plan filed</li> <li>• Gate in message but wrong delivery location</li> <li>• Shipment substantially exceeds scheduled ETA</li> <li>• Driver loss of contact (carrier report)</li> <li>• Driver loss of contact (system report)</li> <li>• Accident or vehicle breakdown (no spill or release)</li> <li>• Spill or release – driver/carrier reported</li> <li>• DHS orange or red threat alert level declaration</li> <li>• Cumulative risk score increase over normal</li> </ul>

<b>Flow of Events</b>	<ul style="list-style-type: none"> <li>• Driver pushes in-cab panic button</li> <li>• CTU receives message via UCI/fleet tracking vendor</li> <li>• CTU passes message to FedTrak risk engine; risk engine spikes risk score and passes score back to CTU</li> <li>• CTU posts score on Security Specialist's desktop and send visual/auditory alerts to Security Specialist</li> <li>• Pre-defined workflow for Security Specialist is invoked by FedTrak – may involve shipper, carrier, state action agencies, and TSA; Security Specialist will follow defined workflow until the situation is fully resolved.</li> <li>• TBD response workflow for a security incident</li> </ul>
<b>Post conditions</b>	<p>Detailed shipment transaction details are stored in the Shipment Transaction Repository. Shippers, carriers, and consignees are able to view data on the en-route shipment and unfolding events re: the driver's panic button alert via their portals. Shippers, carriers, and consignees are able to retrieve data on the transaction after it is completed via their portals.</p> <p>FedTrak will create and store a complete record of the incident from the time the panic button alert is received until the incident is fully resolved. Security Specialists actions and communications are stored in the FedTrak Operations Repository.</p>
<b>Alternate Flows and Exceptions – other scenarios</b>	Dependent on response workflows tbd.
<b>FedTrak Schematic Reference &amp; Data Flow</b>	Not applicable
<b>Assumptions</b>	None
<b>Issues</b>	None



# **Appendix A**

FedTrak Project Team Meeting Work Product

# VIP ~~PRESIDENT~~ SCENARIO

Intelligence  
OFFICER

Schedule  
START  
END

LOCATION  
POINT w/  
Shape boundary

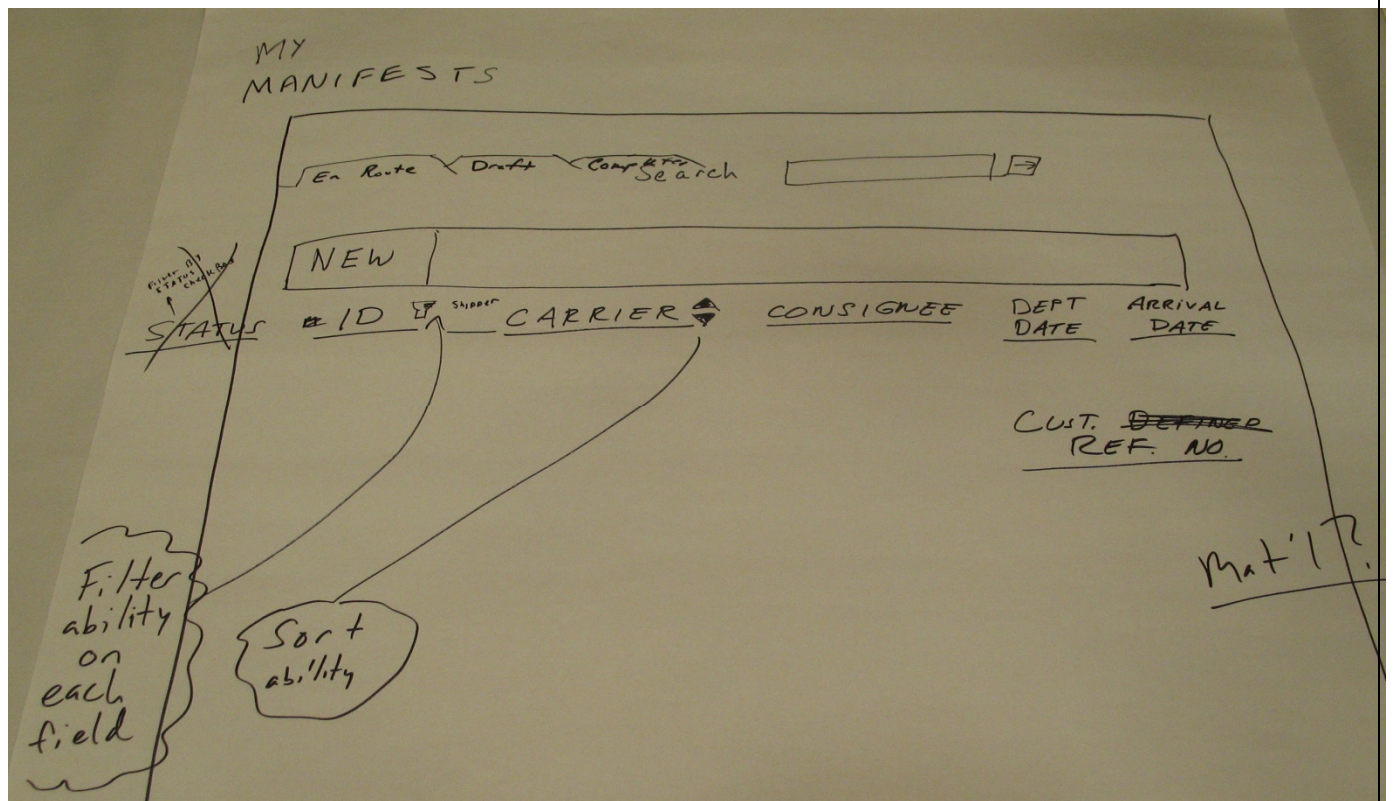
QUERY  
Show TRIPS  
That intersect  
DURING Schedule

SAVE TO  
CREATE  
monitoring  
Tool

DISPLAY  
Active Routes  
Planned Routes  
Template Routes  
TRIP History

EXCLUSION (Y/N)

ACTIONS:  
Re Route  
NOTIFY upon  
Proximity



# Scenario 1 - HP

- ✓ 1.1 Shipper Registers
- ✓ 1.2 Carrier Registers (Shipper / Carrier /
- ✓ 1.3 Consignee Registers (Consignee))

- ✓ 2.1 Shipper Drafts E-manifest for new ships manifest
- ✓ 2.2 Shipper ~~manages~~ <sup>manages</sup> E-manifest (Update / Edit / Delete) Schedule

- ✓ 3.1 Carrier creates Profile Updates (My Fav routes)

- ✓ 3.2 Carrier <sup>edits manifest &</sup> selects route for manifest (alt route ~~alt route~~)

- ✓ 3.3 Route validation (system)

- 3.4 Carrier modifies a default route / draws new route

- 
- 4.1 Gate Out / Custody Change  
- validate / initial risk score

- 4.2 Position reports / Modify Risk Score / view "Events" on security desktop

- 4.3 Gate In

- 4.4 Custody Change / Off Load / Complete Manifest

## Unknowns / Risks

- Non Functional Requirements
  - Security
  - Performance
- Roles
- Permissions
- Shipper Permit for shipments (i.e.)
- Master data list for Tier 1; how maintained
- Route monitoring methodology
- CPL database / frequent driver change
- Validate carriers on hazmat materials
- Shipper specifies route
- Optimistic vs. pessimistic locking
- Initiation for finalization of manifest

# GLOSSARY

---

MANIFEST:

ATOMIC UNIT

- DESTINATION

- ~~CARRIER~~ Specific by Shipper  
& CARRIER

- Possibly many per TRUCK

Bill of LADING:

SCAC - 4 digit code unique to CARRIER

TRIP - Anything that happens between gate-out

Multiple manifests/shipments and gate-in

Tracking of a summary manifest

EVENT - Message received that ~~no~~ causes  
risk score to be re-analyzed

# SCENARIO 1- Happy PATH

## 3.1 Carrier creates Profile / FAVORITES

CARRIER

~~ADD~~  
Create  
FAVORITE

Shipper  
Consignee

Primary  
Route

Alternate  
Route

Would  
Clone really  
be "SAVE AS  
TEMPLATE"

MATERIAL

- ID
- QTY ?
- PACKAGING

NAME  
user defined

EDIT

FAVORITE  
Settings

Delete  
Template

## Other Scenarios — Track

- President / High change rate Geofence
- Load rejection
  - Partial
  - Full
- Panic (before gate out / between gate out & gate in / after gate in)
- Off route
- TSA Alert
  - route specific
  - material specific
  - company specific
- Alternative Route(s)
- Track Breakdown - / Hand Off
- Intelligence Analyst Input
- Gate IN never received
- Multiple 'events' at same time
- Construction on route / accident / detour
- Shipper / Carrier / Consignee do not match
- GPS signal not received as expected
- Risk profile score over threshold (numerous factors)
- Hijack
- Truck wrecks with spill
  - No Associate Manifest on gateout
  - No gateout <sup>as expected by</sup> ~~manifest~~ ETO on manifest
  - ~~No gatein~~ Registration does not match as
    - projected late delivery - based on current location and estimate of time to get to destination
  - Risk scoring / Geofence drives up location rule needs
  - unexpected separation → need to track trailer

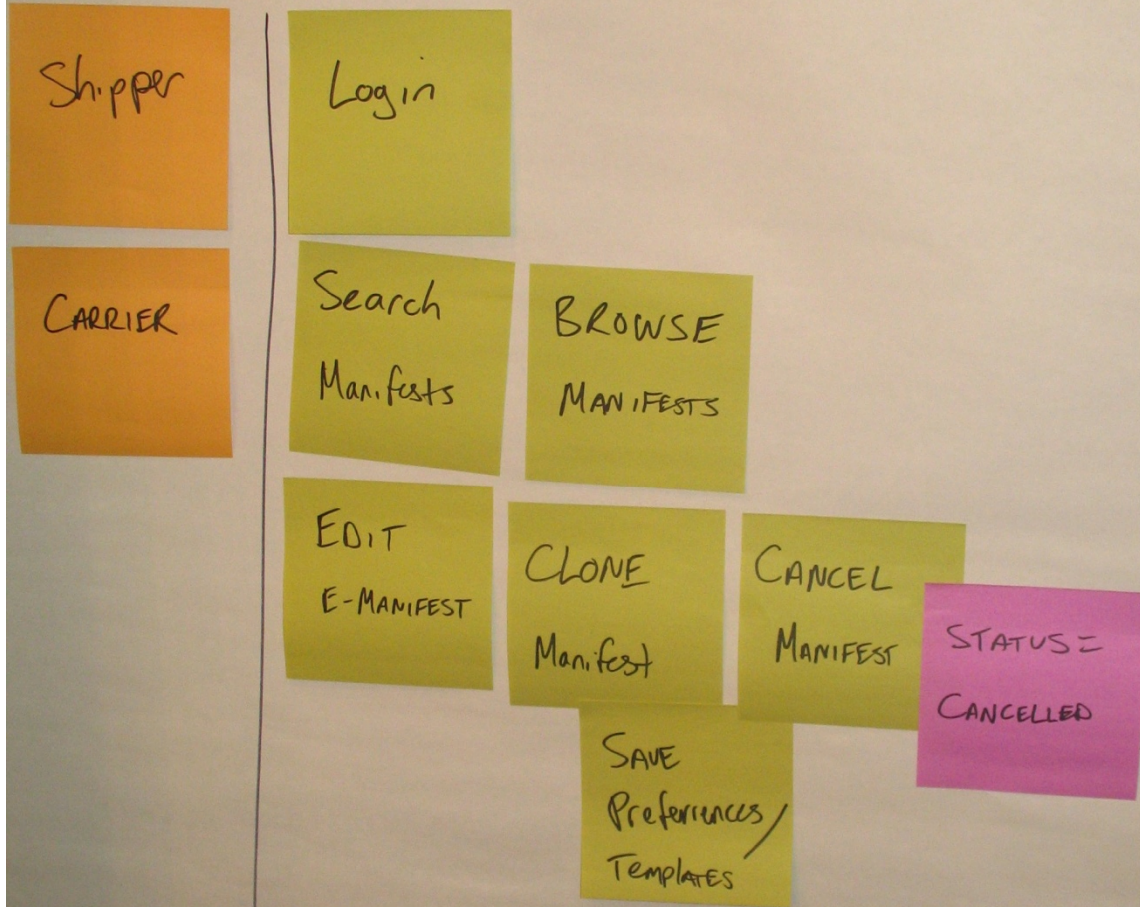
as near to truck

### Paperwork/System

- draft manifest not used
- various internal system errors
- shipper wants to determine route
- draft manifest ≠ actual
- \* - gate out received w/o finalized manifest
- \* - driver does not sign / does not gate out / starts drive

# Scenario 1 - Happy Path

2.2) CARRIER/  
Shipper Manages "my manifests"



# Scenario 1 - Happy Path

4.2 Progress / Modify Risk Score / View Events

Security  
Specialist

Ops  
Manager

Intelligence  
Analyst

Risk  
Score

Risk  
Score color  
&  
Status

SUMMARY  
MANIFEST  
- CAR - TRUCK  
- DRIVER  
- MATERIALS

TREND  
of  
Risk  
Score

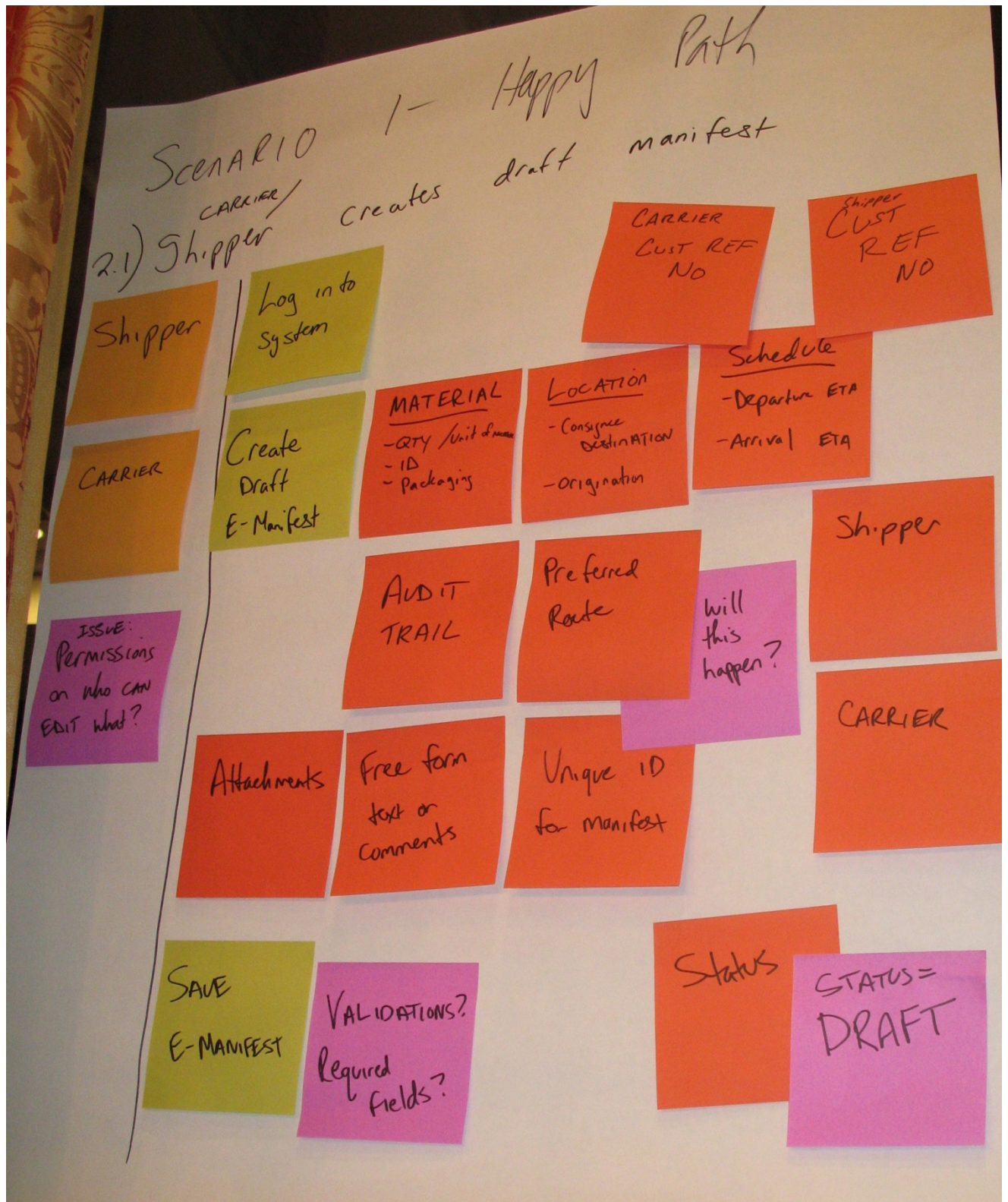
LAST Known  
location  
&  
Time stamp

Potential  
Population  
Density

REACT TO  
ALERT

DRILL Down  
to investigate  
A TRUCK

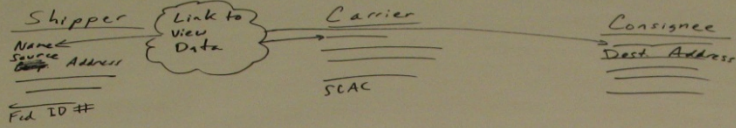
SEND INFO  
TO OTHERS



# MANIFEST DETAILS (VIEW)

Manifest ID — Status: En Route

Print Edit Clone ~~Void~~

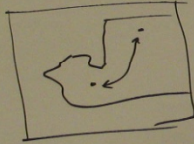


## Materials

Qty	UoM	Code/Description
-----	-----	------------------

## Route

123  
—  
—  
—



## Electronic Envelope

MSPS 723 ~~723~~

ON **NEW** — choose a template a standard manifest

OR

last manifest for

Consignee ☐

Shipper ☐

Equipment?  
Alternate routes?

Created by — on —

Modified by — on —

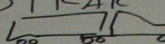
# SUMMARY MANIFESTS

☒ EN ROUTE   ☐ DRAFT   ☐ COMPLETED   ☐ READY TO SHIP

Search

ID	DEPT DATE	ARRIVAL DATE	CARRIER	SHIPMENTS	CUST REF
127	7/2	7/7	ACE TRUCK	SHIPPER - CONSIGNEE • DOW - ACME MUNITIONS • DOW - ABC CHEM	- 123 - 456

## ROUTE PLANNING

FEDTRAK 

DATA LAYERS

☐ UNLOADED 1  
☒ Loaded  
☐

MAP

TOOLS  
       
 SEARCH LOCATION

MY ROUTES

EDIT ATTRIBUTES  
 COMMON NAME  
 SHIPPER  
 CONSIGNEE  
 DEFAULT? ☐  
 TEMPORAL DATA

# Scenario 1 - Happy Path

## 1.3 Consignee Registers

Consignee

Ability to  
Pre-Register?

Log in  
Name &  
PW

Assume  
(for now)  
Consignee &  
Shipper are  
different entities

Assume  
Approx  
?  
Tier 1  
Consignee

Consignee  
enters  
Registration  
Details

NAME,  
ID

LOCATION

Contact  
Details  
- Address  
- contact details  
- emergency contact

Materials  
they  
Accept  
by ID

Assume  
Master  
data lookup  
(list of materials  
updated somehow)

Authorized  
users &  
Roles

Registration  
is  
Approved

Consignee  
manages  
registration  
info

# Scenario 1 - Happy Path

## 1.2 - Carrier Registration

Carrier

Ability to  
Pre-register?

Login  
Name &  
PW

Assume  
Approx

Carriers for  
TIER 1

Carrier  
enters  
Registration  
INFO

Name,  
Unique ID

Contact Details

- Headquarters
- Address
- email / phone
- emergency contact

How do we  
manage an  
emergency contact  
"tree" structure?

Assume  
no  
integration to  
validate driver  
info

DRIVERS/  
crew

- Name
- CDL
- Citizenship

Conveyance

- Make
- Model
- Color
- Plate

Equipment

- Trailers
- Containers
- SMART TRUCK  
Vendor info

Preferred  
Shipper

- ID
- Name

Authorized  
Users  
&  
Roles

- ADMIN  
- Create / Edit  
Manifest

~~Preferred~~  
Licensed  
MATERIALS-

What Tier 1  
am I allowed to  
carry?

Preferred  
Consignee

- ID
- Name

APPROVE  
CARRIER  
Registration

How CAN  
I validate  
What a carrier  
can carry?

How CAN I  
validate driver  
info?

How CAN  
I validate  
TRUCK / Equipment?

CARRIER  
Manages  
Registration

# Scenario 1 - Step 1.1

## Shipper Registers

Shipper

Ability  
to Register  
is Approved?

Do we  
need this  
step? Some  
Kind of  
Security needed

Log in  
Name &  
PW to  
access Registration

Assume  
one time  
Event per  
Shipper

Shipper  
enters  
Registration  
Details

NAME,  
Federal  
IDENTIFICATION

Authorized  
USERS &  
Roles  
Access/control list

- ADMIN Role
- create Manifest
- Delete Manifest
- others?

Assume  
Approx  
1,000  
TIER 1  
shippers

LOCATIONS

Contact  
Details  
- Address  
- Phone  
- Emergency contact  
- head quarters

BANKING  
or  
FINANCIAL  
INFO

Assume  
Shipper is  
mandated to  
Register

MATERIALS  
that they  
Ship (by 10?)

LIST OF  
Preferred  
CARRIERS  
- Can NOT browse  
- Enter SCAC code

How is  
this done?  
- SCAC code?  
- name?  
- Don't see  
entire list

Assume  
initial  
registration  
is super  
user

Registration  
is  
Approved

Risk:  
How do we  
Approve a  
Shipper?

System  
VALIDATION?  
Automated?

Shipper  
manages  
Registration  
Details

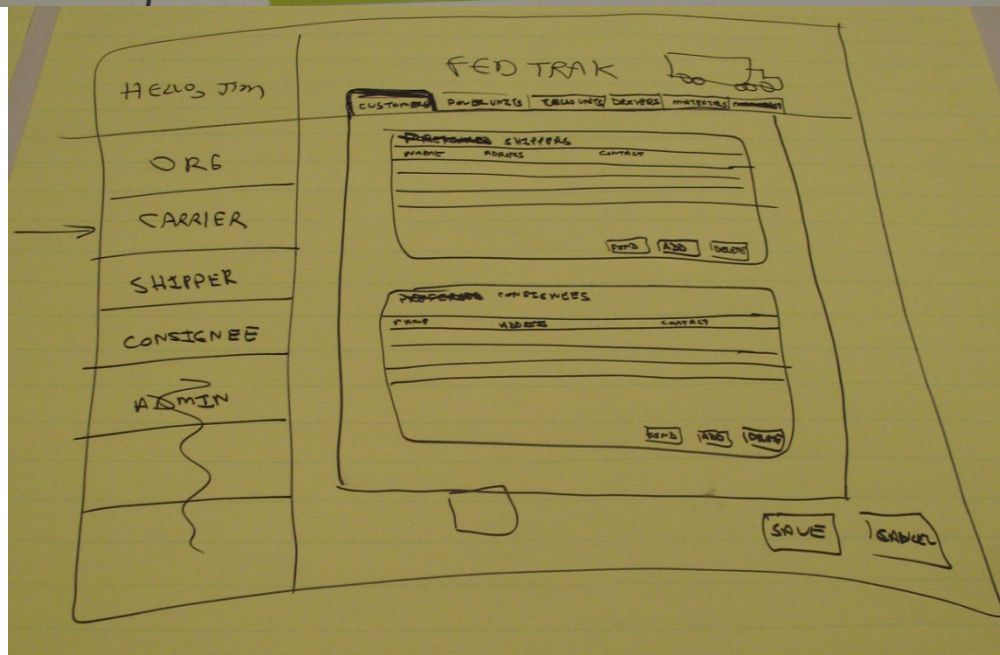
# SCENARIO 1 - Happy PATH

4.2 - Progress / Risk scoring / view EVENTS

Security  
Specialist

Monitor  
TRUCKS

MAP  
VIEW



LOGIN → Register  
~~↓~~

HELLO, Jim

~~ORG~~ FEDTRAK

ORG

NAME   
LOCATION   
TEL#   
EMS TEL#

EMAIL   
FAX

SHIPPER  
☒

CARRIER  
☒

CONSIGNEE  
☒

SAVE

CANCEL

HELP

# ACE TERMS

---

## MANIFEST

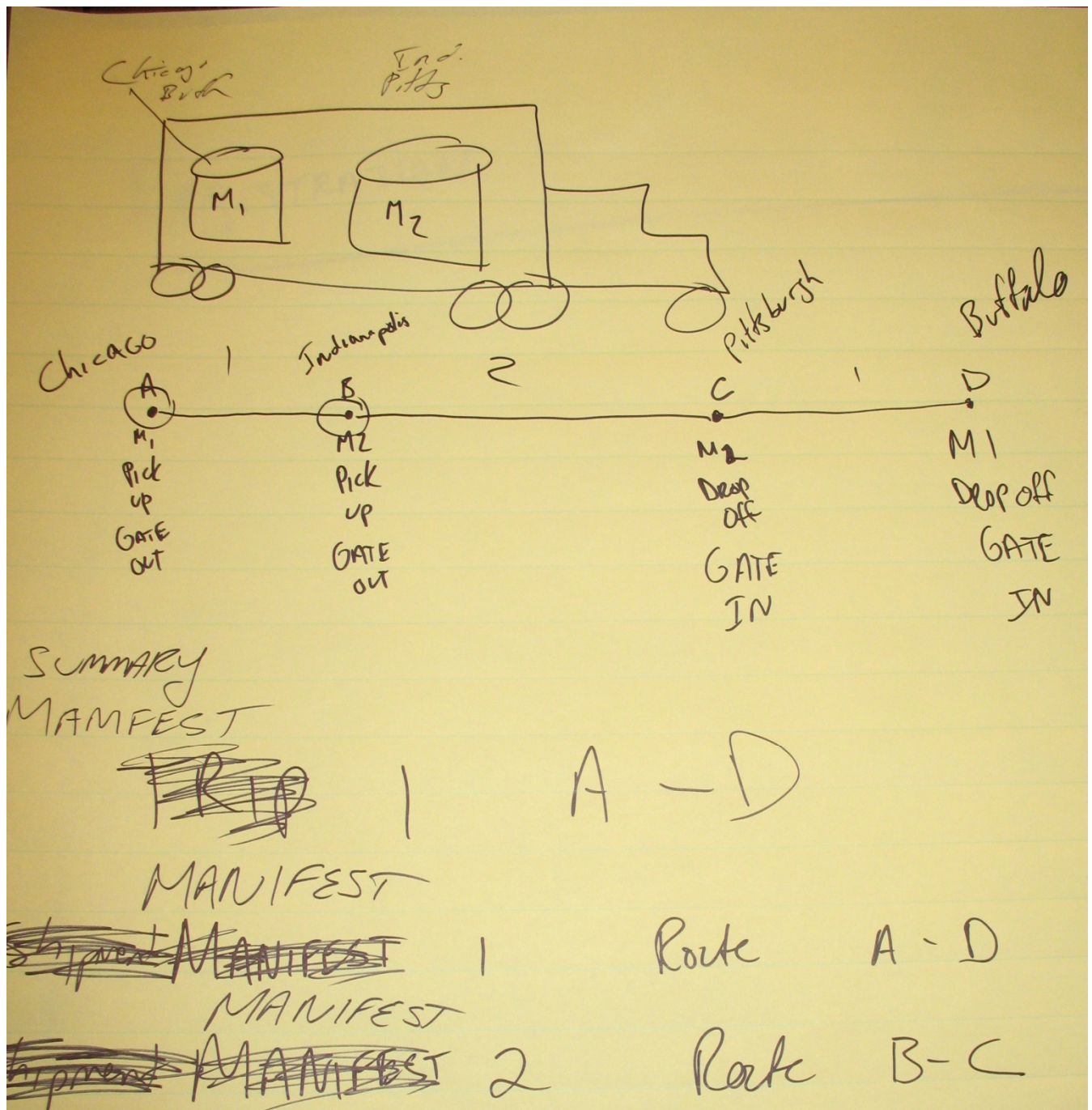
SHIPMENT 1

SHIPPER - CONSIGNEE - MATERIAL

SHIPMENT 2

SHIPPER - CONSIGNEE - MAT'L

ROUTE



# Scenario 1 - Happy Path

3.4

Define New Route / Edit EXISTING ROUTE  
On a manifest

CARRIER

Edit  
Default  
Route

Validate  
change  
in Rate  
(geo-fence registry)

Alter  
Rates or  
mid-points

Assumption:  
ESRI  
GIS Tools

Create  
New  
Route

Validate  
change in  
Rate  
(geo-fence registry)

START  
LOCATION

Destination  
LOCATION

Alter  
Routes or  
mid-points

SAVE  
As New  
Default Route  
to Re-USE

Upload  
existing Saved  
Routes

DRAFT — Ready to Ship — EN ROUTE — Complete — VOID

Summary  
Consolidated Manifest?

My TRIP

Security Specialist only

See Events PRINT SUMMARY MANIFEST VOID ADDIT TRAIL

STATUS: DRAFT

TRIP ID: 123-4-5

CARRIER:

=====

START LOCATION:

123 MAIN ST  
Chicago, IL  
Aug 1, 2009

FINAL LOCATION

345 BROADWAY  
Buffalo, NY  
Aug 20, 2009

SHIPMENT MANIFESTS

ID	Shipper	Consignee	MATERIAL	QTY	GATE OUT TIME	GATE IN TIME	STATUS
123	DUPONT	Alpha Corp	Phosgene	10 lbs	Chicago 8/1	Buffalo 8/20	DRAFT
345	DOW	Beta Corp	Chlorine	5 gallons	Indianapolis 8/5	Pittsburgh 8/12	DRAFT

ADD

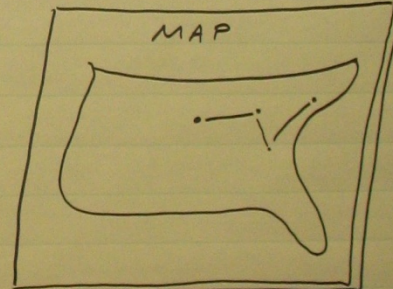
ROUTE

NAME	ORDER	REMOVE
"WINTER ROUTE"	1	<input checked="" type="checkbox"/>
"SUMMER ROUTE"	2	<input checked="" type="checkbox"/>

Route Creation/Exit Screen

SUGGEST ROUTE ADD

MAP



TRIP DETAILS

DRIVER CREW TRUCK TRAILER

CANCEL

SAVE

Picked up

DRAFT — Ready to Pickup — ~~Ready to Pickup~~ — EN ROUTE — Delivered

DRAFT / ~~Ready to Pickup~~ / Signed  
EN ROUTE / Delivered

Shipment ~~Manifest~~ <sup>MANIFEST</sup>

STATUS: DRAFT

Shipper

NAME

Address: \_\_\_\_\_

GATE OUT:

CARRIER

NAME

Address \_\_\_\_\_

GATE IN:

Consignee

NAME

Address \_\_\_\_\_

MATERIALS

QTY	Unit of Measure	Code / Description	Delete
20	lbs	Phosgene	<input type="checkbox"/>

(ADD)

Electronic Envelope

Document	Description	Delete
M12SN	A desc of something....	<input type="checkbox"/>

(ADD)

DIGITAL SIGNATURES

	Shipper	CARRIER	Consignee
<del>Not for</del> Pickup			
<del>Not for</del> Delivery			

(CANCEL)

(SAVE as DRAFT) (Submit)

## My Shipments

SHIPPER

MATERIAL

DATE

Search

	<u>ID</u>	<u>SHIPPER</u>	<u>MATERIAL</u>	<u>QTY</u>	<u>STATUS</u>
<input checked="" type="checkbox"/>	125	DUFONT	Phosgene	10	DRAFT
<input type="checkbox"/>	869	EMPIRE	Hydrogen	5	DRAFT
<input type="checkbox"/>	523	BAXTER	GAS	2	DRAFT
<input type="checkbox"/>	467	LASRO	Nuclear Waste	1	DRAFT

# Scenario 1 - Happy Path

3.2 / 3.3 CARRIER updates MANIFEST

CARRIER

Log into  
System

Select  
Route -  
PRIMARY

Select  
Route -  
Alternates

ASSUME:  
VALIDATE  
Route

Assume  
Primary  
&  
2 Alternates

Select  
- DRIVER  
- Crew

Enter new  
DRIVER

DRIVER  
ID

Select  
Equipment  
- TRUCK  
- TRAILER

Enter new  
Equipment

TRUCK ID

TRAILER ID

Enter  
Seal

Seal  
Number

# **Appendix B**

## **DOT/EPA Manifest Roles and Responsibilities**

<http://www.epa.gov/fedrgstr/EPA-WASTE/2005/March/Day-04/f1966.htm>  
Federal Register March 4, 2005

**ENVIRONMENTAL PROTECTION AGENCY**  
**40 CFR Parts 260, 261, 262, 263, 264, 265, and 271**  
**[FRL-7867-4]**  
**RIN 2050-AE21**

Hazardous Waste Management System; Modification of the Hazardous Waste Manifest System

AGENCY: Environmental Protection Agency.

ACTION: Final rule.

Pages 10792-10794

4. Offerors and the Preparation of Hazardous Waste Shipments and Manifests. The proposed rule would have added a new definition of "preparer" to the definitions in 40 CFR 260.10. While this new definition was proposed in the context of those using an electronic manifest, the purpose of the definition was to extend to the electronic manifest sufficient flexibility to enable the person performing the steps necessary to prepare a waste shipment for transportation to also prepare and sign the electronic manifest on behalf of the generator.

The discussion in the NPRM of the proposed "preparer" definition referred to the instructions for Item 16 of the current manifest paper form as a precedent for this flexibility in the paper context, since the Item 16 instruction allows signatures on the generator certification statement to be made "on behalf of" the generator. Thus, this aspect of the proposed rule raised an issue dealing with the activities of shipment preparers, their authority to initiate and sign the manifest for the generator, and their resulting responsibilities.

Similarly, in the context of TSDFs rejecting waste shipments and preparing manifests to forward rejected waste to alternate facilities (or return the shipment to the generator), the NPRM raised the issue of the responsibility and liability of the rejecting TSDF when it initiates a new manifest and signs the generator's certification statement. For the latter issue, we proposed that the TSDF in such cases was signing the manifest in the capacity of an "offeror" of the shipment, but we asked for comment whether the TSDF forwarding a rejected waste under a new manifest should be viewed instead as signing the manifest as the agent of the generator. Today's final rule affirms that the TSDF rejecting waste and completing a new manifest to track the rejected waste to an alternate facility (or the generator site) signs the manifest in the capacity as offeror of the shipment, and not as an agent of the generator. Nor would the TSDF be functioning as a generator by initiating such a manifest, although the NPRM would have had the facility sign the Generator's Certification statement. The specific issue of TSDFs rejecting wastes and their offeror responsibilities when they complete and sign new manifests is addressed in detail in section IV.B.3. of this preamble. However, because the offeror concept carries broader implications for hazardous waste shipments and waste handlers, and overlaps with the "preparer" concept that we proposed in the May, 2001 NPRM, we are including additional discussion here of the offeror status and how it impacts more generally those who prepare hazardous waste shipments and manifests for transportation.

The term "offeror" refers to a status that is well understood under the Hazardous Materials Regulations (HMRs) of the Department of Transportation (DOT). The HMRs apply to persons who transport hazardous materials in commerce, as well as to persons who offer hazardous materials for transportation. Since hazardous wastes are also hazardous materials within the scope of the HMRs, and since our RCRA statute requires us to regulate hazardous waste transportation-related activities consistent with DOT regulations, the requirements and policies adopted in the HMRs with respect to those who offer hazardous materials for transportation ("offerors") apply to hazardous waste shipments and those who offer hazardous wastes in transportation. DOT consistently has interpreted the "offeror" status as connoting those persons involved with performing certain "pre-transportation" functions that must occur before hazardous materials are transported in commerce. Over the years, DOT has described the pre-transportation functions that may be performed by an "offeror" as including activities such as determining a material's hazard class, selecting a packaging, making and labeling a package, filling a hazardous materials package, preparing a hazardous materials shipping paper (including the hazardous waste manifest), providing emergency response information, and certifying that a hazardous material is in proper condition for transportation in conformance with the HMRs. The latter certification is in fact made when one signs the shipper's certification on a hazardous materials shipping paper, which occurs with respect to the hazardous waste manifest when one signs the Generator's Certification statement. DOT has issued interpretive letters and policy statements respecting offerors and their responsibilities when they perform the types of pre-transportation activities described above. However, these activities and responsibilities were further clarified by DOT when the Department codified these policies in a recent final regulation dealing with the applicability of the HMRs to loading, unloading, and storage. See 68 FR 61906 (October 30, 2003). In this rule, DOT codified a new regulatory definition of "pre-transportation function," and listed the above-described activities and others as examples of these functions that are specified in the HMR and "required to assure the safe transportation of a hazardous material in commerce." See 49 CFR

171.8.

In the preamble discussion of the "pre-transportation functions," DOT explains that a pre-transportation function is performed to prepare a hazardous material **and its accompanying shipping documentation** for transportation and is required to assure its safe transportation in commerce. [68 FR 61906 at 61909](#). The rule further explains that it does not matter if the pre-transportation function is performed by the shipper's (generator's) personnel or by the carrier's (transporter's) personnel. The HMR requirements apply to any person who performs or is responsible for performing the pre-transportation functions, and that person must perform the functions in accordance with the HMRs. See [68 FR at 61909-61911](#). Moreover, as to when compliance or non-compliance must be demonstrated, DOT has stated that it would generally expect an offeror to be able to demonstrate compliance with all applicable pre-transportation requirements at the time the hazardous material is staged for loading and the shipping paper is signed, as this is the offeror's certification that the material has been prepared properly for transportation in accordance with the HMRs. *Id.* at 61911-61912. At the same time, however, DOT has clarified that "intermediaries" who certify as the offeror assume responsibility only "for all aspects of that shipment about which he knew or should have known."

EPA is today clarifying that the issues concerning the activities of shipment "preparers" and the corresponding issues tied with the authority of a generator or other preparer to complete and sign the Generator's Certification statement on the manifest are governed by the same considerations discussed by DOT with respect to "offerors" and the performance of the pre-transportation functions described in 49 CFR

171.8. Since hazardous waste shipments and waste handlers are subject to the HMRs, and DOT recently has finalized a rulemaking under the HMRs which provides more clarity on these issues, EPA is deferring to these DOT requirements, rather than adopting its own definitions or differing interpretations based on the "on behalf of" language in the manifest instructions or on "preparer" signatures, etc.

Therefore, this final rule resolves the issues pending in this rulemaking relating to preparers signing manifests and TSDFs initiating new rejected waste manifests consistent with the DOT requirements in the HMRs pertaining to offerors and pre-transportation functions. Moreover, we have amended the Generator's Certification statement on the manifest form so that it will be described on the revised form as the Generator's/Offeror's Certification. This change more accurately represents the fact that the person signing the certification statement may in some instances be an offeror involved with the preparation of the waste shipment (or of the manifest) for transportation, rather than the waste generator.

While the proposed rule discussed the offeror status while dealing with the issue of TSDFs rejecting and re-shipping wastes, we wish to emphasize that the offeror concept is broad enough to cover many waste shipment scenarios. Indeed, the offeror status and signature would be encountered most commonly in connection with the waste pick-up and transportation arrangements made between generators and waste transporters when the transporters service the generators' sites. Since the transporter's personnel frequently will aid generators in preparing their waste shipments for transportation (e.g., selecting packages, labeling containers, filling and closing containers, selecting and affixing placards, completing the manifest or reviewing it for compliance with the HMRs and RCRA), the transporter performing such pre-transportation functions may be an offeror with respect to the shipment. **While a generator may certainly sign the generator certification statement in its capacity as the generator, today's rule is intended to clarify that another person, such as a transporter making a waste pick-up and helping with the pre-transportation functions, may sign the certification statement on the manifest in their capacity as an offeror.** This person may sign as an offeror if they have performed pre-transportation functions, and can certify that the shipment has been properly described, classified, packed, marked, and labeled, and is in all respects in proper condition for transportation under the applicable international or national regulations. The person preparing the shipment and making the certification is responsible for the proper discharge of the offeror functions they perform and the truth of the certification statement. **The offeror is liable in its independent offeror capacity for discharging their offeror responsibilities,** regardless of whether or not they may also be viewed as performing these activities "on behalf of" or the agent of the generator, as the generator's independent service contractor, or pursuant to a course of dealing with the generator.

Because we believe that the "offeror" approach and the new regulatory requirements in the HMRs concerning pre-transportation functions deal effectively with the issues we raised in the NPRM with respect to shipment preparers and manifest signatures, we are not finalizing the definition of "preparer" we proposed for inclusion in Sec. 260.10. Nor are we expanding or otherwise modifying the meaning of the language in the Item 16 manifest form instruction enabling one to include the words "on behalf of" in connection with a signature, although it will now apply both to generator and offeror signatures. A preparer who assists with pre-transportation functions under the HMRs, and who can certify to the "shipper's certification" statements in the Generator's/Offeror's Certification, may sign this certification and initiate the manifest as an offeror. The "on behalf of" language is retained in the instruction to the signature item in order to effectuate the limited purpose for which this language was added in

1986, that is, to connote that generator (and now offeror) organizations typically act through their employees or agents, and that the employee/agent signatures bind the organizations they represent.

The term "offeror" thus connotes a status in hazardous materials management distinct from that of a shipper or generator. The offeror's responsibilities are limited to the proper discharge of the pre-transportation functions they perform or certify to being properly performed. While it is true that a generator may often elect to perform the pre-transportation functions, these represent only a subset of the full generator responsibilities set out in 40 CFR part 262. Likewise, when an entity other than a generator (e.g., transporter or TSDF) performs pre-transportation functions as an offeror, it does not thereby assume full generator responsibilities. Rather, it assumes only the more limited responsibilities (for the pre-transportation functions) and the distinct liability that attaches to the offeror status. Therefore, a TSDF that only is offering hazardous waste in transportation after rejecting and staging the waste temporarily at its facility would be subject to the offeror responsibilities for the new movement of the waste, but it would not be subject to the full range of generator requirements. This issue is explained further in section IV.B.3. of this preamble.

<http://www.epa.gov/fedrgstr/EPA-WASTE/2008/February/Day-26/f3615.htm>

**Federal Register**  
**ENVIRONMENTAL PROTECTION AGENCY**  
**40 CFR Parts 260, 261, 262, 263, 264, 265, and 271**  
**[EPA-HQ-RCRA-2001-0032; FRL-8534-1]**  
**RIN 2050-AG20**

Hazardous Waste Management System; Modification of the Hazardous Waste Manifest System

AGENCY: Environmental Protection Agency (EPA).  
ACTION: Notice of data availability and request for comment.  
February 26, 2008

EPA agrees with waste management industry and state government commenters' concern that it would not be efficient to have an electronic manifest system collecting data only from electronic manifests, while another paper-based system addresses the data only from paper manifests. Therefore, we believe that the system being designed should be a unified system for processing and distributing data from all manifests, including data from paper manifests. We considered several options aimed at simplifying the process for collecting paper forms and at ensuring that the data collected from both electronic manifests and paper forms could be efficiently processed so that a comprehensive set of manifest data would be available to users and regulators. We have identified a preferred approach that we believe provides the most efficient solution to the dual paper/electronic systems problem.

Under our preferred approach, the final destination facility (i.e., designated final TSDF), for each hazardous waste shipment involving a paper manifest, would be required to submit the top copy (i.e., Page 1 of the 6-page set) of the paper manifest form to the e-Manifest system operator within 30 days of receipt of the waste shipment. While the e-Manifest system is not yet designed, we envision that the designated facility could mail a copy to the e-Manifest system operator or could transmit an image file to the EPA system so that the e-Manifest system operator could key in the data from the paper copies or image files to the data system. Alternatively, the designated facility could submit both the image file and a file presenting the manifest data to the system in image file and data file formats acceptable to the e-Manifest system operator and supported by the Central Data Exchange (CDX). For paper copies mailed to the system by designated facilities, the e-Manifest system operator would create or obtain an image file of each such manifest, and store it on the system for retrieval by state or federal regulators. The e-Manifest system operator also would key in, electronically scan using an optical character recognition (OCR) device, or otherwise transfer the federal- and state-regulated waste data from these paper copies to the e-Manifest system. By having all manifest data in electronic form, EPA could extract any data regarding RCRA hazardous wastes for inclusion in its data systems, while the states could pull off data from the system concerning both federally regulated RCRA and state-regulated wastes for processing in the states' own tracking systems.

We envision that designated facilities would be required to pay a fee to the system operator for processing the data from these final copies of the paper forms, and the fee would presumably vary with the type of submission (mailed copy, image file, or image plus data file), as these submission types would likely present a different level of effort insofar as the processing steps required to enter the form data into the system. It is likely that the fee paid by the designated facility would be passed on to the generator (i.e., the designated facility's customer). We estimate that the paperwork burden cost to TSDFs for submitting a copy of the final manifest could be \$1.95 per paper manifest, for an incremental (i.e., over current baseline) annual cost to TSDFs of between \$1.6 million and \$6.5 million per year. In addition, we estimate the possible fee that EPA's e-Manifest system operator (or other EPA-designated e-Manifest affiliate) might charge TSDFs for receiving paper manifests and for transferring (i.e., imaging and keypunching) paper manifest data to the e-Manifest system, could be between \$0.25 to \$0.75 per paper manifest, for an incremental (i.e., over current baseline) annual cost to TSDFs of between \$0.2 million and

\$2.9 million. On a combined basis, we estimate these two components of paper manifest processing incremental costs to TSDFs could total between \$1.8 million and \$9.4 million annually, representing an average incremental cost to TSDFs of \$2.20 to \$2.70 per paper manifest. We invite public comment on our approach and the cost estimates.

We believe such an approach simplifies manifest copy submissions for the regulated TSDFs, who in the future would only need to provide designated facility copies to one location--the national centralized e-Manifest system--rather than supply copies to the numerous state agencies that now collect a copy of the final manifest. Further, it focuses the federal collection effort on a copy of the final paper manifest forms from the designated facilities, which provide the best accounting of the quantities and types of hazardous wastes that were actually received for management. We believe that providing a means to collect a complete set of hazardous waste receipts data from RCRA TSDFs (the merged set of paper and electronic manifest data), also may in the future provide EPA with the means to replace biennial reporting by TSDFs of waste receipts data with a much simpler approach that relies upon the designated facility data reported to the e-Manifest system.

We also believe that there are a number of benefits of this approach to state programs. As states are connected to the e-Manifest system through EPA's National Environmental Information Exchange Network, they would be able to pull off the image files and the data keyed from paper manifests from this central processing service, just as they would be able to obtain the data and presentations of electronic manifests from the eXtensible Markup Language (XML) schemas and stylesheets transmitted on the e-Manifest system. This national data system also presents a much more efficient approach that can eliminate the need for discrete state systems designed to capture manifest data.

In addition, as the e-Manifest system operator would be able to assess appropriate fees for the paper processing and data entry activities necessary to process the data from paper forms and enter them into the e-Manifest system, the actual costs of providing these services would be recovered by the system operator from the designated facility. Since we expect that electronic manifests will be much more efficient to process than paper forms, the differential fees that are established for paper and electronic manifest processing likely would operate as an additional incentive for the transition to electronic manifests.

While we intend to clarify in the final rule that the use of the electronic manifest format would be optional for members of the regulated community, our preferred approach to collect a copy of the final paper manifest forms from designated facilities and to process the data from these paper forms centrally means that these designated facilities will be required to interact with the e-Manifest system (i.e., submitting data either electronically or by mail and paying established fees). Thus, this NODA confirms our intention to have a single national hazardous waste database.

Facilities that elect to use the electronic manifest format would submit their manifest information electronically as a natural consequence of participating in the e-Manifest system. The e-Manifest system would be designed for the purpose of distributing electronic manifest data among the users and regulatory agencies, while the electronic manifest information is being obtained, processed, and transmitted electronically via the e-Manifest system. On the other hand, those facilities and hazardous waste handlers that choose to use the paper manifest forms or are presented with paper forms rather than electronic manifest formats, would need to process the paper manifest forms physically in the conventional manner that has been the norm since the uniform hazardous waste manifest form was introduced in 1984. However, in place of sending a copy of the final manifest directly to the destination state, the final rule would require the designated facility to send Copy 1 of the paper manifest form to EPA's e-Manifest system operator. Thus, the designated facilities would be required to submit a copy of the final manifest to the e-Manifest system, either in the supported electronic format or as a paper copy, and pay a fee for this service. In other words, the use of the electronic manifest format would be voluntary under the final rule, although the submission of either a completed paper or electronic manifest to the EPA system operator and payment of an associated fee in every case would be required of designated facilities. Once this requirement is effective, and all copies of the final manifest (electronic or paper) from designated facilities are being submitted directly to EPA's e-Manifest system operator, the states would be able to obtain their copies of the final manifest and data from the e-Manifest system through their computer systems on the National Environmental Information Exchange Network. It is EPA's intent that the submission of the final paper manifest copy to the e-Manifest system would replace the requirement to supply paper manifests directly to the states. Since the states would have nodes in place on the Exchange Network for receiving manifest copies from the system, it would no longer be necessary for the states to require the direct submission of paper copies to the states. Thus, the paper copy submission requirement could replace the requirement for facilities to submit copies of the final manifest to the states. Note that the facilities that receive paper manifests will still need to retain a paper manifest copy among their own facility records for the 3-year record retention period in accordance with current requirements. We request comment on our recommendation to collect a copy of the final electronic and paper manifest forms from designated facilities and to process the data from these forms centrally.