

“Trust But Verify”<sup>1</sup>  
President Ronald Reagan, 1986

A National Strategy to Mitigate Threats to  
Container, Port and Global Supply Chain Security



PORT OF ENTRY INSPECTION TECHNOLOGY  
INFRASTRUCTURE PROJECT

PHASE II FINAL REPORT

**MARCH 2003**

Submitted by:  
Lawrence G. Mallon, Task Manager  
Program Element 1.14, Fiscal Year 2001  
PROJECT NUMBER 07 243 001

Submitted to:  
Center for the Commercial Deployment of Transportation Technologies  
California State University, Long Beach Foundation  
6300 State University Drive, Suite 332 • Long Beach, CA 90815 • 562.985.7394

This program has been funded by the Center for Commercial Deployment of Transportation Technologies (CCDoTT) at California State University, Long Beach.

Project 07243 001 CCDoTT FY 2001 1.14  
Task Name: Port of Entry Inspection Technology Infrastructure Phase II

---

<sup>1</sup> Dovyai, no provernai from an old Russian proverb cited by President Reagan on occasion of signing Nuclear Disarmament Treaty with the former Soviet Union

# Table of Contents

Executive Summary .....	ii
Prototype Facilities .....	ii
<b>I. Introduction.....</b>	<b>1</b>
A. Guiding Principles .....	1
B. Structure and Use of this Report .....	2
<b>II. The Current Inspection Context.....</b>	<b>3</b>
A. US Customs Initiatives .....	3
B. The Impact of the New 24-Hour Rule .....	3
C. Customs Trade Partnership Against Terrorism (C-TPAT) .....	5
D. Sea Cargo Targeting Initiative .....	6
<b>III. Inspection Technologies.....</b>	<b>7</b>
A. Electronic container seals .....	7
B. Imaging Technology .....	9
C. Materials Detection Technology .....	10
D. Benchmarking Inspection Technology Performance .....	11
<b>IV. Proposed Strategic Seaport Inspection Planning Model.....</b>	<b>15</b>
A. Inspection Technology Layer .....	17
B. Artificial Intelligence Layer.....	18
C. Supply Chain Security and Risk Management Upper Layer .....	22
<b>V. Recommendations and Next Steps .....</b>	<b>26</b>
A. Prototype Inspection Facility .....	26
B. Prototype Port-wide Command and Control Center .....	27
C. Alameda Corridor Prototype Rail Container Security Portal .....	27
D. Moving the Strategic Seaport Inspection Model to Reality .....	28

## Executive Summary

The urgency to develop a framework for seaport cargo inspections has intensified. The possible repercussions of an incident in a major urban area are significant. For example, in addition to the potential loss of life, the Conference Board recently estimated that a dirty bomb detonating in the Los Angeles port complex would shut down the port for eight days and take an additional 92 days to clear, resulting in a \$58 billion dollar impact on the domestic economy.

At the same time, businesses and transportation providers are wary of potentially obtrusive and time-consuming inspection processes. The global and US marketplaces depend on efficient, timely and cost effective goods movement. Accordingly, the research team addressed the question:

How can existing and emerging technologies best be integrated into the seaport inspection process to maximize detection effectiveness without adversely affecting overall throughput volume?

The result is a framework – the Strategic Seaport Inspection Planning Model – that expands outward both temporally and spatially to encompass “pushing out the borders” to origin ports and upstream to the supply chain point of origin. The Model proposes three layers:

- An agile a risk management approach to a global supply chain vulnerability assessment;
- A data, information, and artificial intelligence layer to identify and neutralize potential threats; and
- An inspection technology layer that blends existing and emerging technologies to efficiently and safely evaluate suspect shipments.

Moving forward, the research team developed two sets of recommended actions to begin implementation of the Strategic Seaport Inspection Planning Model:

- Develop a prototype inspection facility, a port-wide command and control center, and a rail portal; and
- Undertake a series of steps to move the Planning Model into reality.

### **Prototype Facilities**

The national prototype demonstration facility can be situated in an area of around 3-5 acres (a candidate site has already been acquired by the Alameda Corridor Transportation Authority). Developed by the Ports, in conjunction with Federal agencies, the facility would be designed to have both road and rail access and would be connected directly to a designated area to unload high-risk containers. The facility would be used by local, state and Federal agencies to examine high-risk containers and respond to container related emergencies. Numerous inspection technologies could be incorporated, such as gamma ray, vapor trace, neutron pulse, UWB, and others in a technology test bed. Information

processing will be accomplished by applying the Customs ACE - ITDS system, interagency common interface consisting of interagency trade data access, and EDI regional database data anomaly review for targeting high-risk containers.

A port-wide Command and Control Center would coordinate the strategic and doctrinal assignment of authority under the port security plan under development by way of operational and tactical guidance via computers, communications and intelligence and computer statistics.

The team also identified a series of research efforts that would be undertaken during Phase III of this project to refine and facilitate the implementation of the Strategic Seaport Inspection Planning Model. These steps, combined with the development of a prototype inspection facility, command and control center and prototype regional rail portal provide a roadmap for ultimately deploying an inspection process that will both improve security and the effectiveness of the supply chain. The Strategic Seaport Inspection Planning Model is consistent with the objectives of the Office of Homeland Security and port authorities and advancing the public/private cooperation necessary to ensure the US security and competitiveness.

## I. Introduction

The urgency to develop a framework and structure for seaport cargo inspections has intensified since the Phase I report for this project was released:

- The November, 2002 report, *America Still Unprepared –America Still in Danger*, issued by the Council on Foreign Relations, calls for a “recalibration of the agenda for transportation security (as) the vulnerabilities are greater and the stakes are higher in the sea and land modes than in commercial aviation. Systems such as those used in the aviation sector, which start from the assumption that every passenger and every bag of luggage poses an equal risk, must give way to more intelligence-driven and layered security approaches that emphasize prescreening and monitoring based upon risk criteria.”
- The Conference Board recently estimated that a dirty bomb detonating in the Los Angeles port complex would shut down the port for eight days and take an additional 92 days to clear, resulting in a \$58 billion dollar impact on the domestic economy.

The Phase I report for this project identified the current state of inspection processes, agency structures, and available technologies. This report addresses the question:

How can existing and emerging technologies best be integrated into the seaport inspection process to maximize detection effectiveness without adversely affecting overall throughput volume?

An entrepreneurial and collaborative inter-disciplinary research team, combining subject matter experts in information technology, transportation, logistics, and artificial intelligence with academic research faculty in management information systems and risk management and civil engineering, conducted the Phase II research effort. The effort was designed to complement the work underway by federal agencies and other research organizations. The result is a proposed Strategic Seaport Inspection Planning Model.

### A. Guiding Principles

The team worked within the context of a radically changed inspection environment and developed a set of guiding principles to frame the research:

- There is considerable potential for the application of artificial intelligence in the form of intelligent collaborative agents monitoring supply chain security. Automated pattern recognition can augment the time-consuming human interpretation, producing better intelligence profiling, investigation, data analysis and targeting, as well as obtaining maximum effective use of inspection technology.
- In the absence of the capacity for 100 percent screening of all containers at both the origin and destination ports, there is considerable merit in

adopting a risk management based approach for adjusting the targeting thresholds based upon vulnerability assessment and threat conditions in which throughput velocity and security, in terms of acceptable risk and confidence levels continuously balanced on a discrete supply chain basis.

- There is increasing concern that the “trusted shipper” concept is fundamentally flawed as the basis for an inspection planning model because supply chains, by definition, are dynamic, rather than static in nature. The degree to which security measures can be embedded in the supply chain varies considerably regardless of written commitment and shipper/ importer certification. In addition, smuggling history suggests that a trusted shipper “fast lane” program will inevitably become an attractive target for penetration, undercutting its effectiveness.

## **B. Structure and Use of this Report**

This report:

- Reviews the current context for inspection processes and deployment;
- Summarizes the technologies that could be rapidly embraced to create a robust seaport inspection process;
- Describes the proposed Strategic Seaport Inspection Planning Model; and
- Discusses the steps needed to implement the Model.

The report provides a foundation of information on a proposed framework for maritime cargo inspections and sets the stage for the next phase of the project – the proofing of the concept. Because of the need for consensus on next steps, the report is also designed for a broad audience of federal and maritime agencies; elected officials and other decision-makers.

## II. The Current Inspection Context

The landscape of the inspection process has changed dramatically since September 11. This chapter summarizes some of the changes in inspection processes and the organization of federal agencies.

### A. US Customs Initiatives

The U.S. Customs Service, now part of the new Department of Homeland Security, has shifted its inspection focus from contraband to weapons of mass destruction (WMD). Accordingly, the agency has implemented a series of initiatives designed to “push the borders out” to the origin - and frequently transshipment ports under its Container Security Initiative (CSI), designed to pre-screen containers for WMD before loading. This, in turn, relies upon the increased accuracy and transparency of trade documentation, in particular the historically unreliable vessel manifests. The CSI seeks to accomplish this objective through

- Adopting a new 24-hour manifest -cargo declaration rule;
- Stationing inspectors at overseas ports; and
- Partnering with shippers through the first-ever supply chain oriented Customs Trade Partnership Against Terrorism (C-TPAT) to extend screening upstream to the vendor at point of origin or consolidation.

In addition, Customs has begun a Sea Cargo Targeting Initiative.

Each of these initiatives and their implications for inspection processes is discussed below.

### B. The Impact of the New 24-Hour Rule

As shown in Figure II-1, the heart of the post-September 11 inspection process starts with the new 24-hour pre-departure vessel declaration. The requirement for ocean-carrier filing of a Vessel Cargo Declaration (Ship’s Manifest) to be filed is mandated under 19 U.S.C. 1431. The requirement stipulates that the declaration be filed 24 hours prior to vessel loading at the origin port (including transshipment ports) with the Customs Service using the electronic Automated Manifest System (AMS). The new requirement replaces a similar filing 96 hours prior to arrival at the destination port. The Final Rulemaking was issued on October 31, 2002, and was effective on December 2, 2002. Failure to file accurate and timely manifests may result in financial penalties and refusal to allow unloading of cargo from container vessels.

The Declaration must contain the following information:

- (1) Shipper’s complete name and address (actual origin of cargo)
- (2) Consignee’s complete name and address (ultimate consignee or cargo owner for “to order” shipments)

- (3) Precise description of cargo or first six digits of harmonized code (“Freight All Kinds (FAK)”, “chemicals” and other generic descriptions are no longer acceptable)
- (4) Quantity, packaging and weight of cargo (“pallets” not acceptable)
- (5) Container and seal number.

A consolidated container that contains five separate less-than-container load shipment, for example, is required to provide these details for all five shipments.

The 24-hour rule is part of the Customs Cargo Security Initiative announced by Customs’ Commissioner Robert Bonner on January 17, 2002, in the form of reciprocity agreements with major container port authority governments involving the stationing of Customs inspectors in origin ports and reciprocal rights to foreign Customs authorities. The Initiative consists of four key elements:

- Establishing security criteria to identify high risk containers (risk assessment);
- Pre-screening high risk containers before arrival at destination ports (data analysis and targeting);
- Using non-intrusive inspection technology to quickly examine high risk containers (screening examination); and
- Developing and using (deploying) smart and secure containers.

What is unstated is whether or not screening examinations will be conducted primarily in origin or destination ports, or both.

To date, agreements have been executed with, or on behalf of, the ports of Halifax, Montreal, and Vancouver, Canada, Singapore, Rotterdam, Antwerp, Le Havre, Bremerhaven and Hamburg. The program goal is to conclude agreements with the top twenty foreign container ports representing over ninety per cent of regular container trade with the top ten U.S. container ports. On June 28, 2002, the World Customs Organization unanimously passed a resolution encouraging authorities representing ports in all 161 member nations to participate in the Initiative.

The implications of the 24-hour rule for the inspection process and overseas inspections include:

- Extending the inspection process upstream in the global supply chain toward the source, or at least first point of consolidation, by requiring accurate shipper supplied data to the carrier pre-departure rather than pre-arrival;
- Pushing the opportunity and timing of meaningful data analysis and targeting of contraband, in particular weapons of mass destruction, identified as high risk containers to a 24- hour window prior to vessel departure;

- Shifting the primary point of inspection using non-intrusive screening examination of high risk containers to the origin port while providing the redundant opportunity for additional secondary examination of high risk containers, and both targeted and random containers at the destination port, and the reverse in the case of exports under reciprocity agreements with origin port authorities;
- Exploiting opportunities for the use of supporting information technology through continuous virtual 100% screening of containers through their trade documentation for contraband of all types, while concurrently improving regulatory compliance, by clearing “exceptions” during the twelve to fourteen day ocean line haul leg avoiding inspection related delays, in combination with real time data sharing among other inspection agencies in advance of deployment of ITDS/ACE environment;
- Affording a dual use opportunity for in transit visibility and supply chain security concurrent improvement through the planned introduction and deployment of electronic container seals;
- Improving trade facilitation, as well as security, by increasing throughput velocity at the destination port by pre-clearing and releasing pre-screened and sealed containers upon arrival.

### **C. Customs Trade Partnership Against Terrorism (C-TPAT)**

C-TPAT is an unprecedented joint government-business voluntary initiative to build cooperative relationships between the ninety percent largest shippers by value and the Customs Service to strengthen overall supply chain as well as border security. C-TPAT participation open to carriers, shippers, and service providers requires the participants to commit to four key elements:

- Conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines developed by Customs and the trade community. The guidelines encompass the following areas: procedural security, physical security, personnel security, education and training, access controls, manifest procedures, and conveyance security;
- Submit a supply chain security profile questionnaire to Customs;
- Develop and implement a program to enhance security throughout the supply chain in accordance with C-TPAT guidelines; and
- Communicate C-TPAT guidelines to other companies in the supply chain and work toward building the guidelines into relationships with these companies.

The noteworthy aspects of C-TPAT are that it is:

- The first direct attempt to address the overall issue of supply chain, as distinguished from merely border security and
- Being developed in a collaborative manner with the import community.

By joining in this first, worldwide, supply chain security initiative, participants will hopefully ensure a more secure supply chain for their employees, suppliers and customers. In consideration of their participation besides the security benefits, Customs offers other potential benefits to C-TPAT members including:

- A reduced number of border inspections (and faster processing times at border crossings);
- An assigned account manager (a segue into the account-based ACE environment);
- Access to C-TPAT membership list;
- Eligibility for account-based procedures (bi-monthly, monthly payments); and
- An emphasis upon self-policing instead of Customs verifications.

#### **D. Sea Cargo Targeting Initiative**

Rounding out the earlier border and supply chain security efforts, in September 2002, Customs Commissioner Bonner announced the Sea Cargo Targeting Initiative to modify the way in which Customs approaches high-risk cargo at commercial seaports. The initiative has three components:

- Improving the Automated Targeting System (ATS) first introduced in 1996 to incorporate counter-terrorism intelligence;
- Ensuring that all vessel manifests (and cargo declarations) are processed through the ATS and reviewed by trained personnel; and
- Standardizing procedures that Customs uses to screen high-risk containers including non-intrusive inspection technology, radiation vapor trace detection, and container seal integrity checks.

### III. Inspection Technologies

The Phase I report for this project provides extensive information on available and emerging technologies potentially applicable to the inspection process. This chapter summarizes three technology sets that have emerged as potential key components of a Strategic Seaport Inspection Planning Model:

- Electronic container seals;
- Imaging technology; and
- Material detection technology.

In addition, the chapter summarizes methods for benchmarking inspection technology performance.

#### A. Electronic container seals

The introduction of electronic seals, combined with a mechanical container security door seal and an electronic identification radio device, shows considerable promise. An electronic seal consists of:

- Electronic housing;
- Cable or bolt seal;
- A unique seal number different for the container number; and
- A battery or power source.

Today, most containers use mechanical seals consisting of bolts or wire cable that provide little, if any, cargo security and no audit trail as to the time and place a security breach occurred. The principal reason that seals have not found their way into general commercial usage is cost. Despite exponential growth in cargo theft prior to September 11, no constituent (including the insurance industry, shippers, and federal government) demanded the introduction of seals as a theft deterrent device or tags to track containers in the manner automatic equipment identification (e.g., Lojack) and similar devices track stolen vehicles. Costs range from \$5.00 for a mechanical seal to several hundred dollars for a sophisticated active reusable electronic seal. In comparison, the average declared value of import containers is in the millions of dollars.

Accordingly, seals provide a simple and relatively inexpensive way to detect intrusion and tampering with contents within a container and to leave physical evidence of the event. Mechanical seals are now giving way to electronic seals that provide physical security, temper evidence, and information management. Electronic seals use radio frequency (RF), infrared (IR) or fiber optics. Seals can be combined with Global Positioning System (DGPS) or cellular phone network for precise geographic location positioning,

Electronic seals can be active or passive. Passive seals are inexpensive (less than \$5.00 USD) and disposable. They can be polled or interrogated by a reader. Active seals are reusable and cost significantly more.

A standard mechanical seal with a data chip can record and store the seal number and other content information. In comparison, electronic seals can store and manage data in memory such as a permanent seal identification number, contents, shipper contact information, and other manifest details such as are now required by the Customs Service. Seals can be read by RF, IF and fiber optic readers. Adding DGPS means the seal can be polled remotely and interrogated real time on specific data, pinpointing the timing and location of intrusion. As yet, there are no international standards for electronic seals. However, the International Standardization Organization (ISO) is in the process of developing such a standard.

From Customs' perspective, introduction of the electronic seal is the missing element that will make the trusted source (the entity that verifies the cargo declaration) and eventually places the seal on the container at the first point of origin or consolidation truly trustworthy. The seal will be read at the in-gate origin port and evidence of tampering will result in denial of entry to the port or marine terminal. The seal will be read again prior to vessel loading. It will be read again at time of unloading at the destination port, and finally before leaving the marine terminal by truck or rail. For in bond movements the seals can be continuously monitored until the container arrives at the ultimate consignee. For in-transit moves, Customs will monitor the seal until the container exits U.S. Customs territory.

Electronic seals from various manufacturers are currently undergoing field-testing in the Northwest under the lead supervision of the Washington State Department of Transportation. The tests involve disposable seals in a cross-border and roadway environment. The seals are similar to mechanical door seals with a battery-powered transponder that can be read by hand-held readers or fixed readers. The seals were linked to ITS tags using wireless DGPS on the truck tractors permitting real time asset location within the region. In those tests the seals have six data fields. One is used for the seal number and another for a unique manufacturers identification number. The other four fields are blank available for other data. Seal data can eventually be linked to electronic data interchange (EDI) standard transaction data messages among supply chain participants. The preliminary tests proved the viability of the seals in an operational environment but did establish a correlation between number of data fields, reader accuracy and vehicle speed with obvious tradeoffs to be considered in the development of national performance standards.

Another similar test was conducted in conjunction with the Alameda Corridor Transportation Authority, facility manager of a twenty-mile, dedicated, below-grade right-of-way for container-unit trains transiting between the fifteen terminals comprising the Los Angeles-Long Beach port complex and the major international rail transfer facilities operated by the BNSF and UP railroads. That test demonstrated the viability of using electronic seals, and seal integrity verification, from the marine terminals to rail transfer facilities using fixed readers with unit trains traveling at speeds up to forty miles per hour.

The Maritime Transportation Security Act of 2002 requires the Secretary of Transportation to promulgate performance standards for electronic seals. It is anticipated that once container seal performance standards are promulgated, Customs will require their introduction in a rule-making procedure. The Act also requires the deployment of automated identification systems and long-range vessel-tracking systems, which by shifting from VHF to satellite communications, such as INMARSAT, will have the potential effect of extending the reach of container seal monitoring from end-to-end of the global supply chain.

Container seals can be a bridge to the future integration of supply chain security with total asset visibility in the ocean line haul segment and the interoperability with domestic intermodal surface transportation. They afford the first real opportunity to wring out the supply chain inefficiencies inherent in extended free time on the part of shippers and absence of real time asset location on carriers and container owners. With the first real opportunity for end-to-end supply chain integration, in the name of supply chain security with electronic seals, and the requirement for trusted shipper certification, emphasis will inevitably shift from the seal to the smart target with on-board sensors. In reality, the shift is merely incremental as reefer and hazardous material (HAZMAT) containers already rely upon on-board sensors and domestic trailers, and rail cars have long had integrated sensor suites.

It is no coincidence that both electronic seals tests sought to integrate electronic seals with real-time location devices continuously monitoring signals from tags placed upon rail cars, truck tractors, and container chassis to provide public and private entities with real-time asset location, equipment management, in-transit visibility, performance monitoring, and enhanced supply chain security. To date, only Matson Navigation, among ocean carriers, utilizes active tags on its dedicated chassis fleet. Despite the fact that the United States is the only major trading nation in which the carriers control chassis equipment, and much of that is done by pooling or leasing companies on behalf of multi-carrier alliances, few chassis, and no containers in the domestic market, utilize automatic equipment identification.

## **B. Imaging Technology**

Gamma ray imaging is the technology now deployed both in origin and destination ports by U.S and foreign customs inspectors (Figure III-1). Its software enhanced, CATSCAN-like, gray-scale images of the inside of containers provide the first real look at the internal stuffing configuration and contents at reasonable throughput speed (120 containers per five-hour watch shift at a marine terminal using portable equipment) or up to forty miles per hour continuous double-stack container scan using a rail fixed portal system without real-time analysis and interpretation. This reflects a quantum improvement over earlier low-energy x-rays dependent upon back-scatter imaging with lower resolution and throughput speed. It is the logical starting point for developing an integrated platform for screening high-risk containers in a high throughput

environment in a transportable or fixed portal configuration such as a rail portal. At an origin port, it provides an immediate verification check of the interior contents and stuffing or consolidation in comparison to the new cargo declaration submitted by a trusted shipper and vessel manifest. It can be used in combination with container seal verification at the gate or the crane prior to vessel loading.

The image accuracy makes it both an anti-theft and (WMD) device detector. It can identify human beings, false compartment, and even misclassification and undercounts with positive offsetting revenue implications. Importantly, for data sharing purposes it lends itself to secure transmission of images for remote interpretation and analysis by other inspection agencies, such as during the ten to fourteen day voyage from origin to destination port affording time for targeting of suspect containers for further screening or physical examination or clearance of “exceptions” prior to vessel arrival.

However, imaging technology has its limitations in that it does not provide materials detection and, at this time, absent automated reasoning requires time-consuming human interpretation. As the Phase I report revealed, the current state of the art is vapor trace detection with known limitations in detection accuracy, false positives, and low throughput rate.

**Figure III-1: Imaging Technology Application**



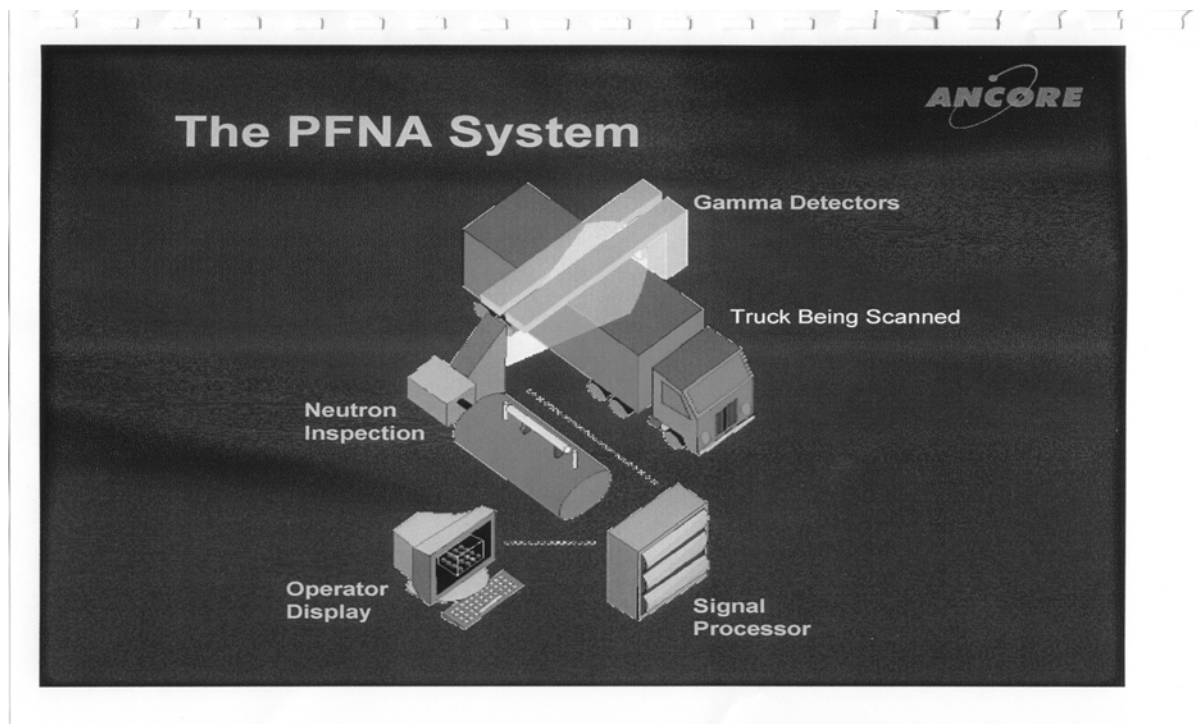
### **C. Materials Detection Technology**

With Federal government research funding assistance, the first of several generations of materials detection technology now appears ready for at least experimental deployment. An example is shown in Figure III-2. Thermal neutron and pulsed fast neutron analysis (gamma-ray based) technology have proven

capable of detecting and classifying contraband drugs and explosives and appears capable of discerning the elemental composition and constituent elements (carbon, oxygen, hydrogen, nitrogen) of a wide range of contraband. Other materials detection and identification technologies, such as ultra-wide band technology (which based upon short-range broad-spectrum radio-frequency wave bombardment) will be available in the future.

In the interim, current materials detection technology can be integrated with imaging technology to detect first explosives and nuclear, chemical and biological weapons smuggled a contraband in sea containers at high throughput origin and destination ports (as a last line of homeland defense/security) preferably at a high risk common inspection facility.

**Figure III-2: Example of Materials Detection Technology**



#### **D. Benchmarking Inspection Technology Performance**

At the heart of the inspection layer of the Strategic Seaport Inspection Planning Model is the ability to optimize the performance effectiveness of inspection technology measured against the degree of risk or vulnerability posed by specific threat type and amount (misclassified goods, contraband, explosives, humans, WMD) with reference to both the probability of intrusion and probability of detection. While many performance factors come into play such as cost, throughput, maintainability, reliability, penetration etc., perhaps the most

important is the ratio of the probability of detection (PD) of a given target measured against the probability of false positive identification (PFP) whereby:

- Probability of Detection (PD) – Given a container with dangerous material inside, what is the likelihood that a scanner will identify it to contain dangerous material?
- Probability of False Positive (PFP) – Given a container without any dangerous material inside, what is the likelihood that a scanner device will incorrectly identify it as containing dangerous material?

The two metrics that will most adversely affect the free uninterrupted flow of commerce – and a potential port shutdown short of an incident - are the overall percentage of containers that must be non-intrusively examined under a given threat level that is in turn dependent upon the performance of pre-screening and targeting, and the PD/PFP ratio.

The level of current inspection technology performance demonstrates the importance of this analytical approach. Imaging technologies are dependent upon the presence of shapes and the ability of the interpreter –e.g., import specialist- to identify trade data anomalies to target containers for non-intrusive examination and the machine operator in turn to interpret shapes to identify the presence of concealed contraband.

In a random search, containers are routinely designated for inspection without any historical or other basis. In a targeted search, containers are designated by inspectors to be suspicious based on historical and other factors and to be inspected. Less than random detection is unsatisfactory but most common in x-ray shape dependent world requiring human pattern recognition

The result is that traditionally random inspection is more effective at PD than targeting under current limited trade documentation, non-automated pattern recognition environmental and pre-artificial intelligence supply chain monitoring conditions. Much of explosives and WMD are not shape-dependent. Conversely, vapor trace technology used to identify explosives and WMD are notoriously high in PD/PFP ratio.

Figure III-3 and III-4 demonstrate current and future directions in improving and benchmarking inspection technology performance as part of the Seaport Security Planning Model. Both charts depict technology performance and optimization curves.

Each is dependent upon threat type, amount, and overall throughput. In each, the x-axis reflects PD and the y-axis PFP. In each, the apex of the x-axis is 1.00 PD and 0 PFP. The mid-line is .50-.50 PD/PFP or random detection. The arrow points in the direction of optimization for any given inspection technology at any given threat level, type and amount.

Figure III-3 reflects where we are today with sub-optimized performance for both imaging and vapor trace technologies. In this environment for any set of

optimization curves, random performance beats targeted performance and high PD/PFP ratios resulting in a sub-optimized performance envelope.

**Figure III-3:**

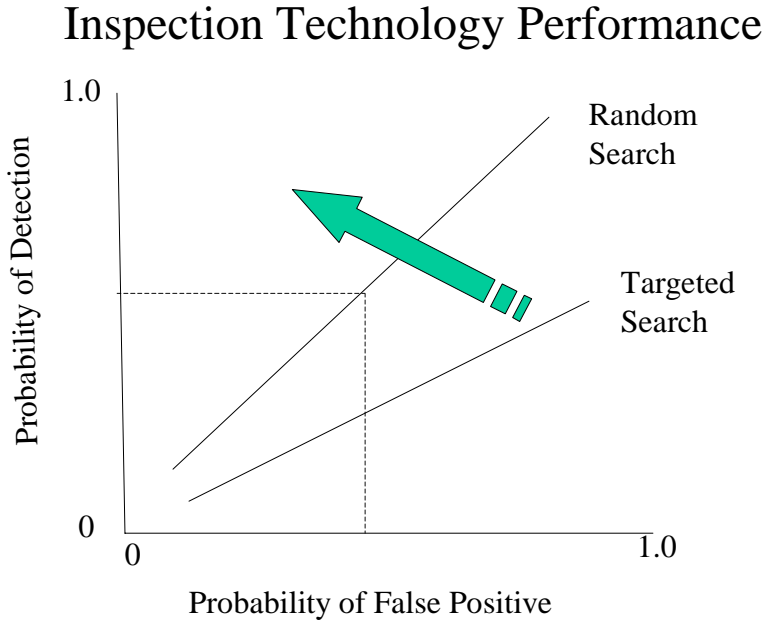
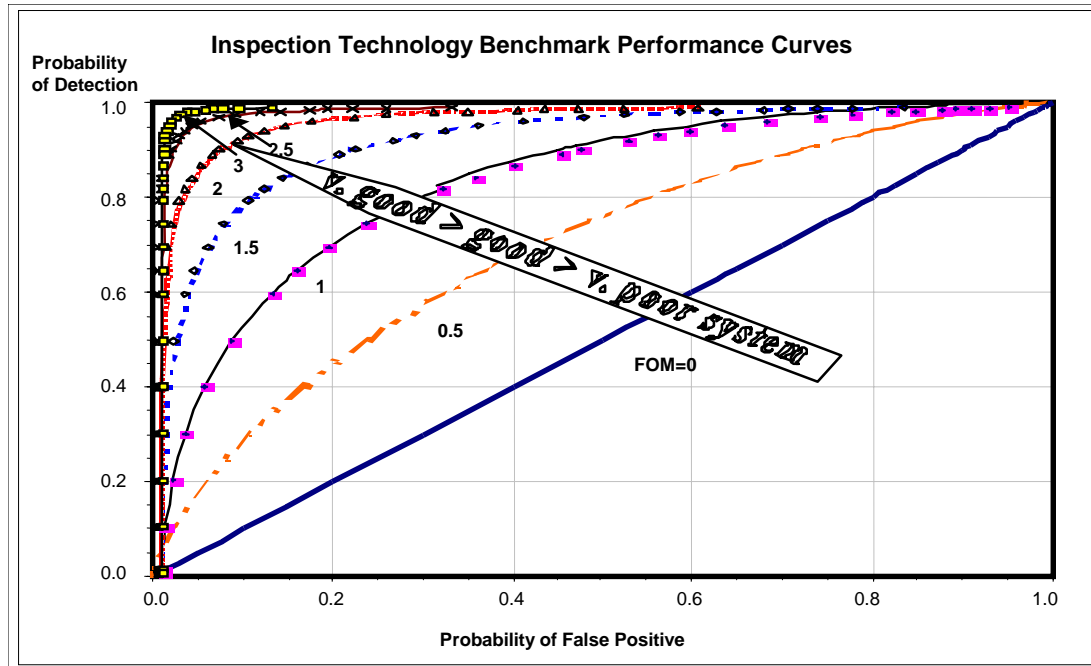


Figure III-4 reflects a range of technology optimization curves incorporating improvements to imaging technology including automated pattern recognition, more robust targeting algorithms, and artificial intelligence, and the introduction of materials detection technology to augment vapor trace and reduce PFP for a broad range of targets.

The arrow points in the direction of an ideal scanner – or suite of scanners along the supply chain sharing targeting and screen imaging data - with no false positives and perfect detection, i.e., upper left corner, whereby Probability of False Positive = 0, and Probability of Detection = 1.0. The broad arrow indicates the direction we need to move in order to improve the performance and deployment of inspection technology along the supply chain from origin to destination port corresponding to targets and threat levels to approach the upper left corner.

Figure III-4:



## IV. Proposed Strategic Seaport Inspection Planning Model

The essence of the proposed Strategic Seaport Inspection Planning Model is to maximize the use and effectiveness of available and emerging technologies from an inspection process perspective and as part of global supply chain, border, and homeland security.

In the evolving information technology-driven Strategic Seaport Inspection Planning Model, the following guiding principles constitute the overall framework within which the proposed approach to goods movement security has been formulated:

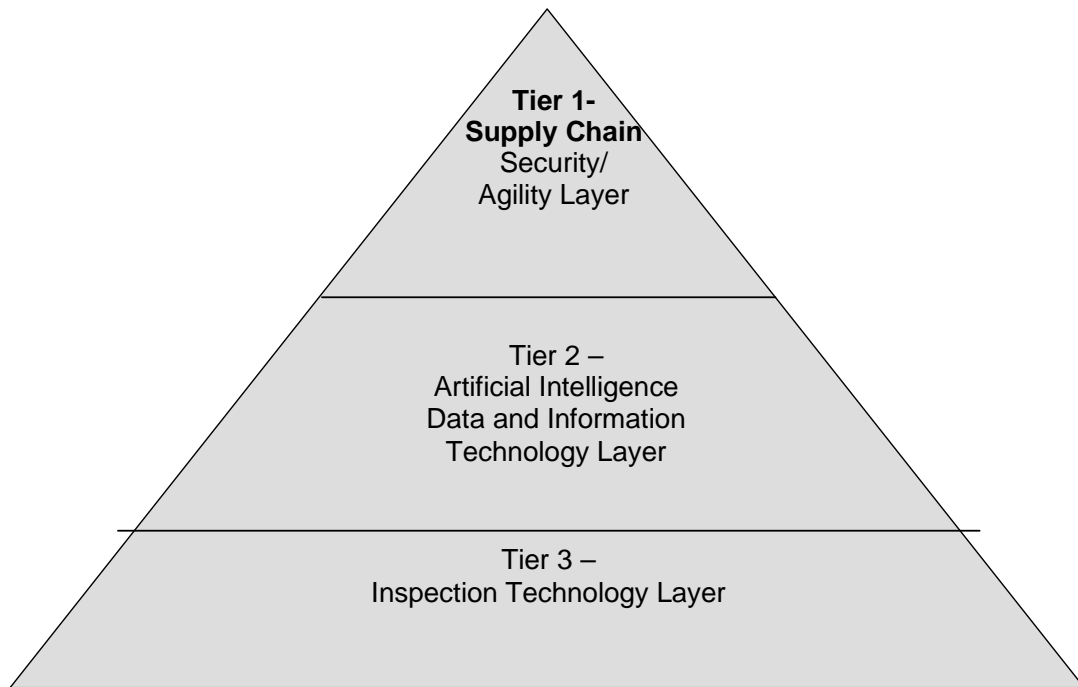
- Move the security process upstream near the source of the shipment (or at least the first point of stuffing and consolidation) and provide incentives for complete, timely, and accurate data;
- Provide physical protection of the in-transit shipment and transportation infrastructure (e.g. container seal standards, real time asset tracking, and in-transit visibility);
- Streamline the point of entry processing, including the provision of express lanes, shipper incentives, and indemnification options;
- Implement shipment and container profiling through data capture and the application of intelligent information management technology;
- Automatically select high-risk shipments and containers for the appropriate level of inspection, by taking advantage of collaborative software agents operating in an information-centric decision-support system environment. At the same time select random inspection samples and dynamically modify the profile building rules used by the software agents based on inspection results using a neural net; and
- Progressively improve physical inspection technology devices with the objective of increasing performance accuracy, reliability and throughput velocity, while decreasing average inspection time and cost.

The research team recognized that ports and border checkpoints are part of the last line of defense in border and homeland security. The decision to inspect or not to inspect a container and the level of inspection should be made well before a shipment reaches the destination port of entry. This is possible only if the full context of the shipment is available for consideration.

As shown in Figure IV-1, the proposed model contains principal layers:

- Inspection technology layer;
- A data, information, and artificial intelligence layer; and
- A risk management supply chain security layer.

**Figure IV-1: The Proposed Strategic Seaport Inspection Planning Model**



The overall model provides:

- Enhanced resolution; and
- An improved confidence level through automated reasoning and artificial intelligence applications.

Each layer is described on page 17.

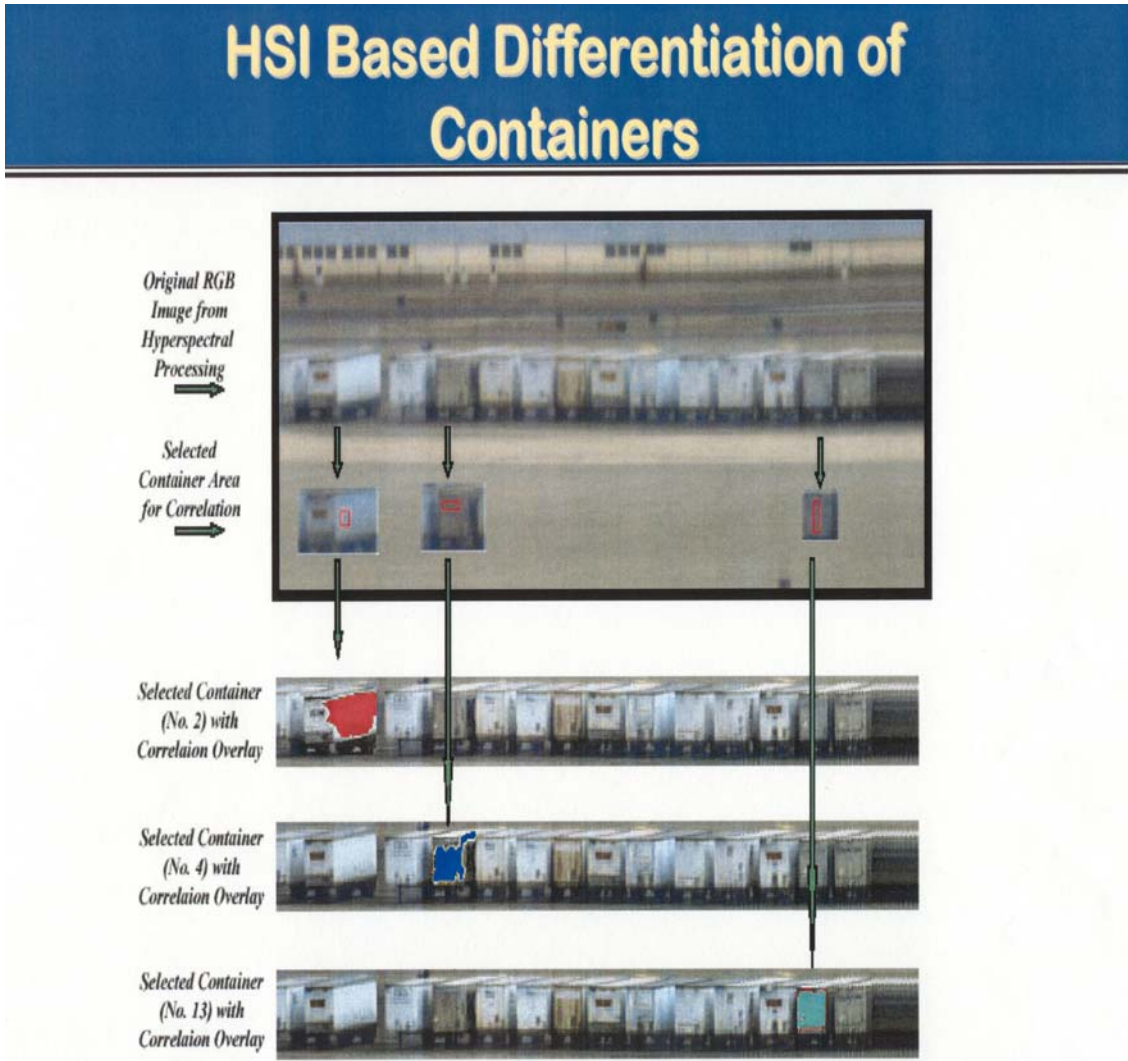
## **A. Inspection Technology Layer**

The inspection technology layer is comprised of imaging and materials detection technology (replacing current vapor trace detection), and supporting information technology designed to create an integrated inspection technology platform for deployment at an origin or destination port, or intermodal transfer facility. Included in the supporting information technology is container seal and overall physical integrity verification, as well as secure data streaming/sharing over the internet. The particular choice of technologies is secondary to the dynamic nature of the threat and technical capabilities. The key components are accuracy, reliability, interoperability, extensibility and minimum adverse impact on commercial cargo throughput velocity.

The inspection technology layer is an integration of available and emerging technologies. The research team determined that the two current technologies – imaging and materials detection – can be integrated using a common gamma ray source with adequate shielding ideally in a portal arrangement in an offset configuration that utilizes a continuous loop wire guided process that guides containers on chassis, rail cars or terminal equipment through the imaging source. In terms of flow process, the type of contraband sought through targeting or random would determine which or both of the two non-intrusive examination technologies would be used on a container or batch basis e.g. gamma ray imaging first for humans and most contraband other than WMD once automated reasoning is deployed for higher throughput levels, and materials detection first for WMD in all instances.

In light of the current and future inspection process and environment, the third supporting inspection (information) technology that can be integrated into a common high-risk, high-throughput inspection platform. The platform would include hyper-spectral imaging using an array of highly sensitive infrared and ultra-violet cameras to provide a three-dimensional, 360-degree view of a subject container in automated operating mode. This technology is capable of not only detecting container seal tampering, but verifying overall container integrity including identifying if the doors have been removed, physical penetration at the corners or bottoms, or altered container number capable of detecting repainting or physical alteration at the micron level. At this level, every sea container is unique and no two are physically identical. Therefore, “before and after” images of each container can be taken at the origin port and electronically transmitted to the destination port for verification at the crane, inspection platform, or in the case of empties or export containers at the gate. An example of the integrated platform is shown in Figure IV-2.

Figure IV-2: Example of an Integrated Inspection Platform



The United States Postal Service, under contract with FEDEX and United Parcel Service for international air and surface mail transportation, is currently utilizing this type of seamless continuous scanning and seal verification process.

### **B. Artificial Intelligence Layer**

At the next level of data and information analysis, the technologies are integrated into the inspection process (including intelligence and profiling, pre-screening and data analysis, and targeting of containers for non-intrusive examination) with the optimum strategy incorporating 100 percent pre-screening, and data sharing for remote analysis and interpretation by other inspection agencies leveraging the use of the inspection technology and achieving virtual rather than physical co-location of inspection functions over the internet eventually through the International Trade Data System web interface for the new Customs account-

based Automated Commercial Environment. Incorporation of an artificial intelligence layer or ontology over the data layer will inject collaborative agents to analyze data, monitor supply chain security by acting as sentinels, and recommend appropriate response in the event of a supply chain disruption. Such adaptive, multi-agent, decision-support systems are currently on the transition path to the military forces in the field.

The collaborative tools within the intelligent information management layer would be specifically designed to address the hypothesis that the “trusted source” concept currently utilized to promote shipment security is fundamentally flawed. Accordingly, a particular feature of the proposed demonstration system will be its ability to adapt to the dynamically changing nature of the security threats that shipments are exposed to. This will require a near real-time feed-back loop between the results of both targeted and random inspection results and the heuristics used by the software agents to build the profiles of individual shipments.

The information technology solution approach to goods movement security relies on the concept of “profiling” all international shipments – the approach utilizes advanced information technology to capture the end-to-end context of each shipment so that software agents operating in a collaborative mode can automatically perform at least the initial filtering, evaluation and profiling functions. In general terms the necessary context includes the data required by Customs and other inspection agencies for clearance purposes, the standardized data used by commerce to process international trade transactions and to achieve efficiency (electronic data interchange), the data obtained through the in-transit monitoring of shipments using AEI and the detection of apparent data or physical anomalies, the relevant law enforcement data on both sides of the border, and at least some elements of national security intelligence.

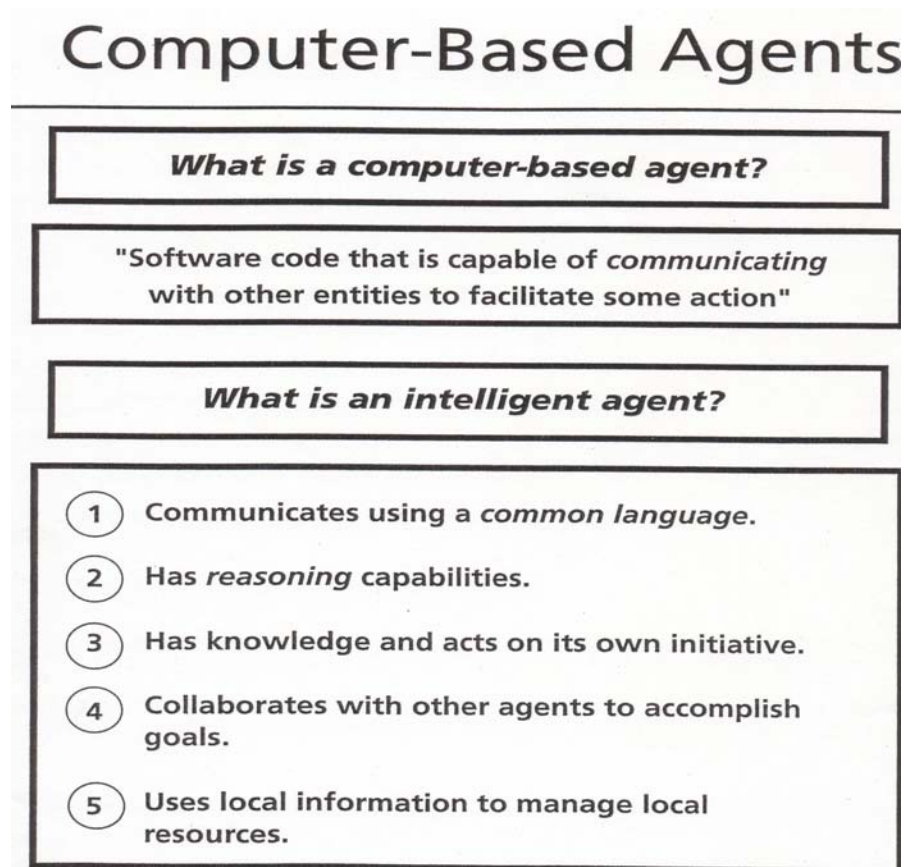
Relevant data collection questions include:

- What kind of cargo does this shipment consist of?
- Where did the shipment originate?
- Who purchased these goods?
- Who sent the shipment?
- Where is the shipment going?
- Who are the shippers on both sides of the border?
- What was the planned and actual shipping route?
- How long has the shipment been in transit?
- Who will receive the shipment?
- What is the history of all parties who touched the shipment?

The focus is on profiling the shipment first, and then the container. Many of the required data elements are already available in existing documents such as: the shipper's Letter of Instructions; the various commercial invoices; the Certificate of Origin; and, the carrier's Bill of Lading. Additional data elements that are needed for building a complete and reliable shipment profile include: financial data (such as letters of credit and bank reports); inland transportation records from both sides of the border; and, in-transit monitoring data for identifying transshipment route changes, delays, and other events.

The proposed technical approach incorporates intelligent agent technology to propose to provide a "shadow staff" of digital assistants to responders and coordinators at all nodes within an extended, distributed, intelligent homeland security network. Information on computer-based agents is provided in Figure IV-3.

Figure IV-3



These assistants analyze and categorize incoming signals and data, and then issue warnings and alerts to specific units as appropriate. The digital assistants manipulate the incoming data within an internal information-centric representation framework to publish statements of implication, and if so empowered, proceed to develop plans for appropriate action. Digital assistants will receive status reports, track shipments, incorporate suitable and available assets in plans, and provide appropriate updates on location and security risks. Others will track the path of incidence and provide appropriate graphic and textual updates for action. Finally, the assistants will manipulate incoming signals, identify significant events (i.e., changes), and modify proposals to meet the changing situation as it develops.

Existing data-centric systems can become clients to such an agent-based system through the use of translators that map the data model in one system to the information model of the other and allow a two way exchange. Such translators have been successfully demonstrated by the Department of Defense in linking legacy data-centric systems to intelligent command and control systems such as the Integrated Marine Multi Agent Command and Control System (IMMACCS) (Pohl et al. 2001). The technology is inherently scalable and allows for the creation and interconnection of multiple object serving communication facilities.

The final element of the data and information layer of the Strategic Seaport Inspection Planning Model is the logical integration of inspection technology output data stream, and trade data anomaly for remote analysis and interpretation, and eventual extension of artificial intelligence to other inspection agencies through the use of the common International Trade Data System (ITDS) front end interface to the Automated Commercial Environment recognizing that the system architecture was designed before September 11 and enhanced security concerns. The system is scheduled to begin deployment in 2004 providing the opportunity for a seaport demonstration coincident with future phases of the project.

The principal elements of ITDS that complement the proposed Planning Model include:

- A common interface that facilitates “pushing” entry clearance and clearance of “exceptions” at the request of other inspection agencies to pre-arrival rather than post-arrival determinations in the case of Customs by the import specialist using a series of red-green, go-no go lights;
- The use of electronic goods and transport declarations designed to integrate all importers and NVOCC’s into the Automated Broker Interface and Automated Manifest System respectively thereby improving the inspection process by eliminating data gaps and expanding electronic data interchange;
- Real-time trade data sharing currently only available to USDA among the forty or more inspection agencies relying upon trade data for profiling, targeting, screening, inspection, and enforcement activities in principal as

early as pre-departure under the 24 hour manifest rule allowing ten to fourteen days for other agencies to screen trade data and origin port inspection technology data output through remote analysis and interpretation prior to arrival and to schedule inspections upon arrival, or pre-clear exceptions prior to arrival thereby reducing delays from cargo holds under current operating practice thereby creating a one-stop virtual inspection process for all border inspection agencies;

- Segregating compliant from high and lower risk non-compliant containers for examination using non-intrusive inspection technology at origin and destination ports; and
- The laying of a foundation for extending the artificial intelligence information layer and application of intelligent agents to other inspection agencies to automate the border inspection process.

### **C. Supply Chain Security and Risk Management Upper Layer**

At the apex of the layered Strategic Seaport Inspection Planning Model is a risk management approach to a global supply chain vulnerability assessment. A similar approach is being used in of the public-private collaborative “Operation Safe Commerce.” No system - even one based upon artificial intelligence and the most efficient use of inspection technology and 100 percent virtual screening of containers -- is going to be 100 percent effective in detecting all contraband even WMD. The research team, therefore, recommends applying risk management to minimize, compartmentalize, emergency response, risk mitigation recovery.

Rigorous analysis must be undertaken to categorize seaport and supply chain security risk into:

- Catastrophic measured into business interruptions on the order of weeks to months;
- Major in which a functional area e.g. troop deployment is temporarily disrupted for a period of days or weeks; or
- Minor in which a transportation e.g. marine terminal or rail intermodal transfer facility is disrupted for a period of days or weeks.

The consequences of any of these events are that firms seek alternate sourcing, distribution, and manufacturing elements. Therefore, a general purpose seaport risk management planning (or diversion) model must investigate the impact of potential disruptions upon regional freight flows, and regional supply chain resiliency, emergency response and recovery planning that in turn is a function of the impact measured by metrics of value, and increased contingency planning, by individual importing and exporting firms and third party logistics firms. This is depicted graphically in Figure IV-4.

The research team intends to collaborate with public and private entities to develop and validate the regional supply chain vulnerability assessment model through case studies, workshops, table-top exercises, and simulations using its Regional Supply Chain Simulation Model to test the resiliency of the regional

supply chain and contingency plans and to refine the metrics to conduct real time supply chain security oversight and monitoring. One obvious use of the model - along with the artificial intelligence overlay component is in a command and control mode as decision support tools for a port complex wide emergency response center in support of the Coast Guard Captain-of-the-port modeled on the Los Angeles County Sheriff's similar center for natural disaster response under the State-wide planning apparatus. This approach would emulate the military's C4-I (command, control, communications, computers, and intelligence) methodology.

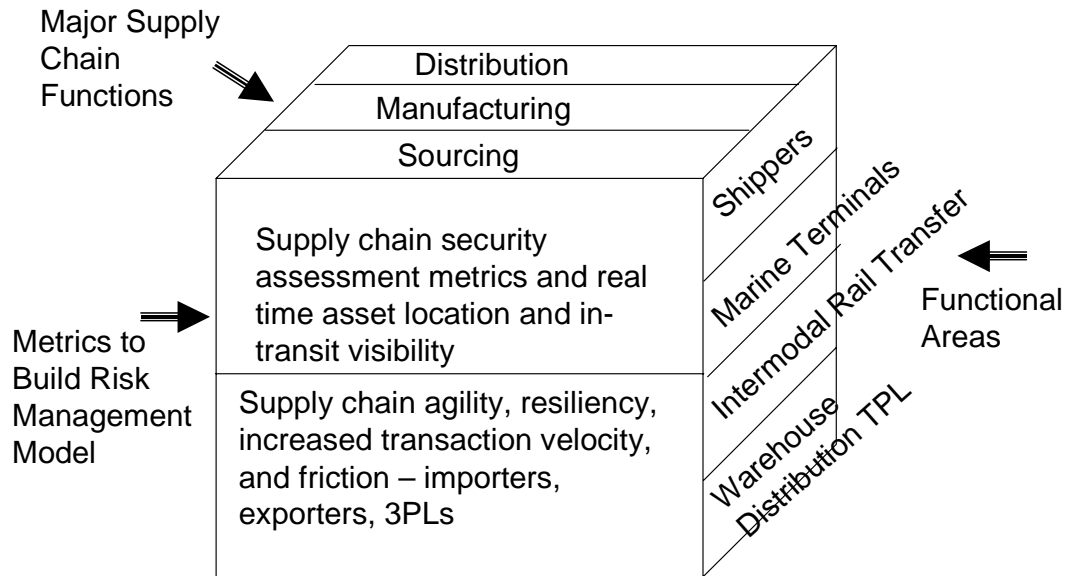
The research team identified that increased emphasis, including more stringent regulatory requirements, will have supply and value chain impacts measured in security assessment metrics as "friction" in those same distribution, manufacturing and sourcing supply chain elements. Increasing supply chain visibility will better reveal the extent of that friction.

The approach, with collaborative public-private strategic partnership, will allow all parties to identify specific vulnerabilities, develop contingency plans, and formulate policies and plans to compartmentalize—and thereby minimize the impacts of supply chain disruptions on the regional supply chain, importers and exporters and the regional and national economy.

In earlier research the research team demonstrated that the more a given supply chain is internally integrated among departments and externally among vendors and suppliers the more efficient and competitive the supply chain. Supply chain security at the micro-level will require a supply chain vulnerability assessment such as is promoted by Operation Safe Commerce and wholly consistent with Customs' Trusted Shipper concept under C-TPATT. This approach initially favors large shippers by value –the very ones targeted by the account driven ACE environment - and later smaller importers as they become more integrated in their internal and external operations.

Figure IV-4:

### 3- Dimensional Vulnerabilities Assessment Model



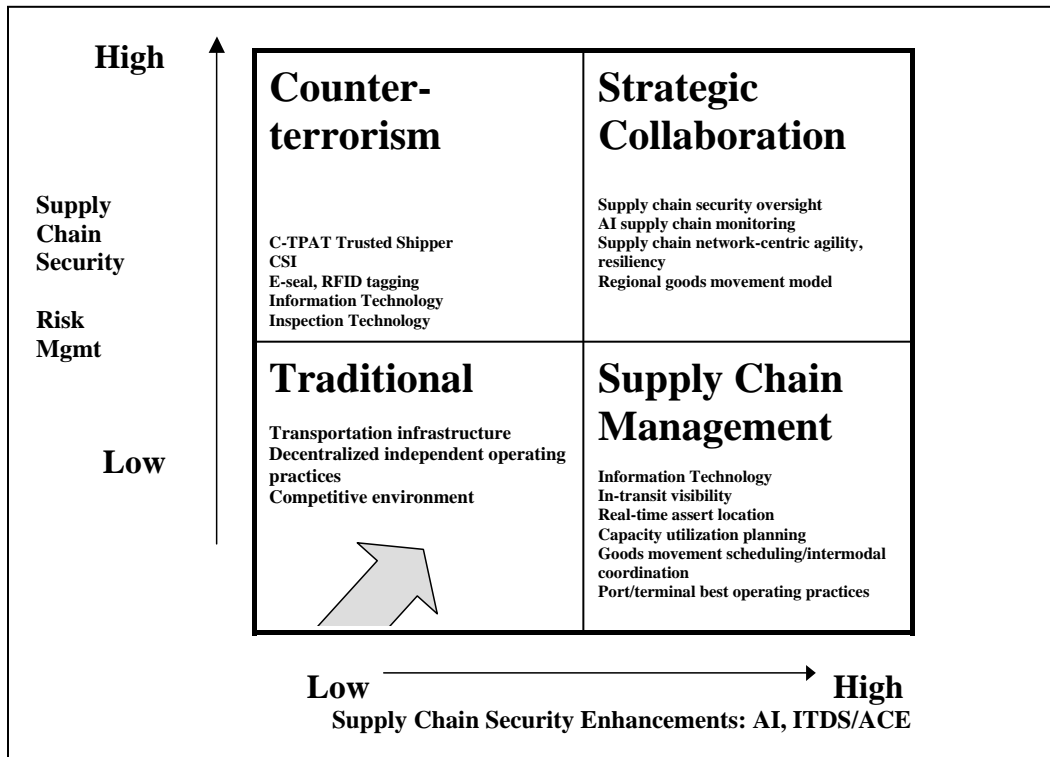
Over time, the emphasis upon supply chain security base upon risk management principles will evolve into supply chain network centric agility with the ability to:

- Sense and interpret risks and opportunities;
- Benchmark and continually track directional indicators that measure operational performance and deviations;
- Encourage collaborative decision making among supply chain partners to make adaptive changes and marshal shared resources including response to disruption; and
- Learn and transform supply chain in response to incidents.

The interplay of supply chain agility and risk management will be employed to first minimize risk, then compartmentalize supply chain disruption, integrate supply chain with regional emergency response systems and contingency planning, incorporate risk mitigation principles, and stress resiliency and supply chain recovery along with transportation infrastructure.

Ultimately, if current trends continue prompted by Customs rulemaking - and the advent of ITDS/ACE - seaport and supply chain security, and supply chain velocity and efficiency measured in visibility, agility and resiliency are in convergence. Improvements in one area - on one side of the equation - will reap corresponding positive benefits on the other side, if friction can be reduced to a minimum (Figure IV-5).

**Figure IV-5: Improving Overall Supply Chain Management and Security**



## V. Recommendations and Next Steps

The context for the inspection process has changed dramatically since the Phase I Report was released. It has also broadened outward and expanded outward both temporally and spatially to encompass “pushing out the borders” to origin ports and upstream to the supply chain point of origin at least in concept. Yet, the inherent flexibility of the layered systematic approach reflected in the Strategic Seaport Inspection Planning Model allows for and anticipates these process changes and those to follow.

Moving forward, the next steps involve proofing the concept of a Strategic Seaport Inspection Planning Model. In that context, the research team has developed two sets of recommended actions:

- Develop a prototype inspection facility, a port-wide command and control center, and a rail portal; and
- Undertake a series of steps to move the Planning Model into reality.

### A. Prototype Inspection Facility

As the port of entry for 35 percent of the nation’s import containers, the Los Angeles-Long Beach (LA-LB) port complex has an urgent need to develop a prototype concept multi-agency and international high-risk container inspection facility. Recognizing this need, the Port of Los Angeles received a \$1.5 million proof-of-concept port security grant from the U.S Department of Transportation for this purpose.

The national prototype demonstration facility can be situated in an area of around 3-5 acres (a candidate site has already been acquired by the Alameda Corridor Transportation Authority) with 6-9 month lead-time for site improvements. Ultimately, the facility would be on a 10 plus acre site accessible to both ports, and away from populated areas. Developed by the Ports, in conjunction with Federal agencies, the facility would be designed to have both road and rail access and would be connected directly to a designated area to unload high-risk containers. It would also be designed to connect with major highways that connect the port to the established distribution sites.

The facility would be used by local, state and Federal agencies to examine high-risk containers and respond to container related emergencies. Agency representatives would be housed on the property and would include the California Highway Patrol, USDA, INS, US Coast Guard, FDA, Customs, DEA, ATF, FBI and foreign customs officials.

Numerous inspection technologies could be incorporated, such as gamma ray, vapor trace, neutron pulse, UWB, and others in a technology test bed. Information processing will be accomplished by applying the Customs ACE - ITDS system, interagency common interface consisting of interagency trade data access, and EDI regional database data anomaly review for targeting high-risk

containers. A model based on Laredo Border crossing can be used in the demonstration.

The property would be bonded and used to house container inspection equipment, to test new inspection methods, and to respond to emergencies. The facility would be available to local law enforcement agencies and would house a joint hazardous material response team from the LA City Fire Department, LA County Fire Department and Long Beach City Fire Department. Space would also be made available for foreign personnel to inspect containers traveling to their countries from the LA-LB Port complex.

The facility can be a prototype for replication in an origin, transshipment or destination port as part of a layered strategy to mitigate threats to container, port, or global supply chain security.

#### **B. Prototype Port-wide Command and Control Center**

Ports are the last line of layered defense against terrorist intrusion using containers to smuggle weapons of mass destruction using the opacity of sea containers as the smuggling conveyance. A port-wide Command and Control Center would complement a common high-risk inspection facility to create a design that will integrate facility access control, a suite of wide area air-surface and subsurface sensors and an interoperable communication network into the planning and design of a new standalone port police headquarters now underway. The Center will coordinate the strategic and doctrinal assignment of authority under the port security plan under development by way of operational and tactical guidance via computers, communications and intelligence and computer statistics (COMSTAT). Accurate timely intelligence and targeted patrols will aid rapid, coordinated, focused deployment. The Center will communicate with the Coast Guard Captain of the Port, all Federal, State and local inspection agencies, including the U.S. Coast Guard, FBI, INS, DEA, U.S. Customs, TSA, the California Highway Patrol, and the Los Angeles County Sheriff's Department Emergency Response Center.

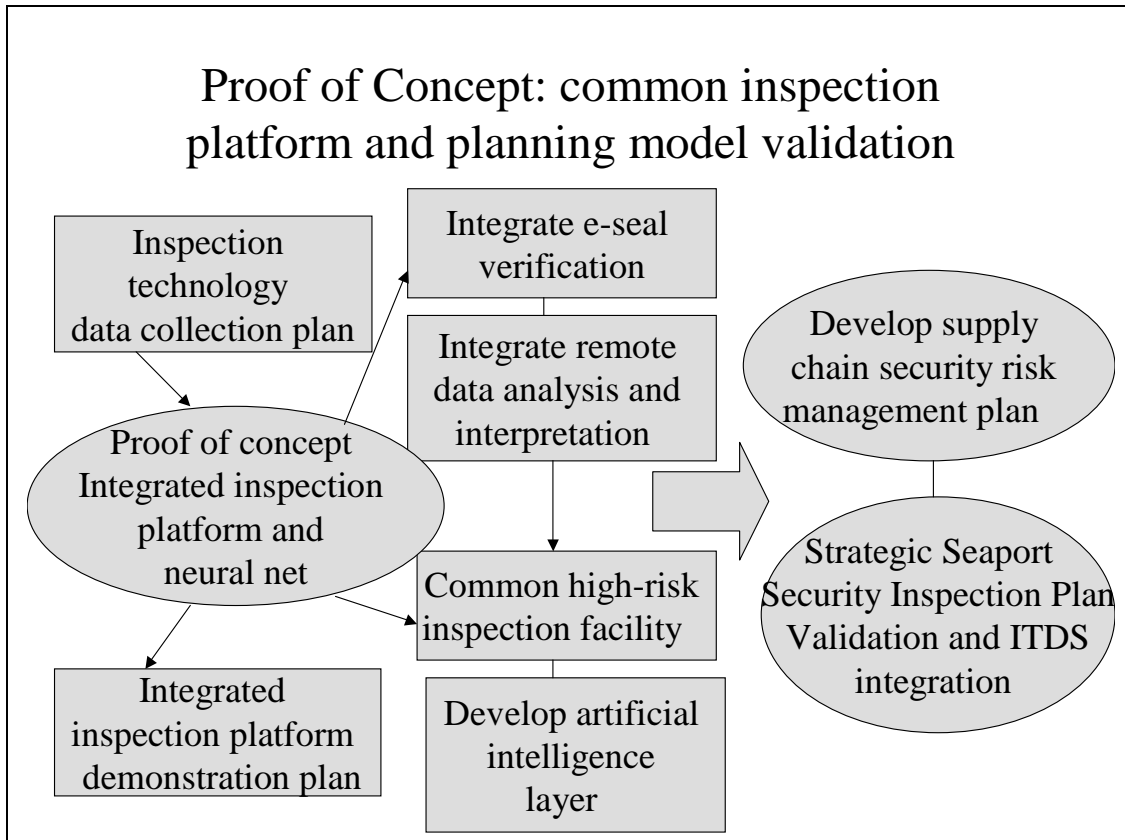
#### **C. Alameda Corridor Prototype Rail Container Security Portal**

The prototype project combines intelligent transportation system and freight management with container inspection to continually monitor rail traffic flow and security. It will assess the feasibility of integrating e-seal reader status with rail automatic equipment identification (AEI), while comparing Electronic data interchange (EDI) and Customs manifest data on individual shipments with continuous non-intrusive examination of double stack containers on unit trains using gamma ray and radiation portal technology. It will capture images and related data for continuous screening examination and targeting into a common database available to authorized users, including inspection agencies, via a secure website or EDI interface. It will provide the conceptual design for integrating information, inspection, and AEI technology, and e-seal monitoring, into a single secure intermodal portal as a prototype element of a layered approach to container security against intrusion from WMD.

#### D. Moving the Strategic Seaport Inspection Model to Reality

The proof of concept approach is also depicted graphically in Figure V-1. The proof begins with Phase III Inspection Technology Infrastructure Project. The Phase III laboratory experiment is central to that effort in that it defines the tangible link between inspection technology and the inspection process. Without better targeting and automated reasoning and pattern recognition the use of inspection technology will be sub-optimized, it will never get better in terms of accuracy, it will not set the course for integration with other technologies such as materials detection as they come along, and it will never incorporate the data sharing potential for remote analysis and interpretation by Customs at origin and destination ports that is the natural segue to data sharing among other inspection agencies using the ITDS/ACE interface.

Figure V-1:



The natural progression for the multi-phased research project is a graduated series of laboratory experiments that builds on the proof of concept of the integrated platform and neural net to incorporate actual target and performance data. Next it integrates electronic seal verification data—and even Automatic Equipment Identification (AEI) data—like the Blaine, Washington experiment perhaps using the Alameda Corridor reader network. Likely it migrates to a distributed demonstration using one or more marine terminals or intermodal rail transfer facilities. It exploits favorable opportunities when they arise such as potential for demonstrating a prototype integrated inspection platform at one or more vendor or port facilities, such as a common high-risk inspection facility in the Los Angeles-Long Beach port complex. The communications and data-sharing element - and eventually common interface - is also central to the inspection model and can be demonstrated among locations or facilities, and eventually among inspection agencies, or at a port-wide command and emergency response center. By 2004 with the phased deployment of ITDS/ACE, a seaport demonstration project may be developed in cooperation with the ITDS inter-agency Board of Directors.

The artificial intelligence component needs to be a high priority when resources become available. It logically follows the neural net and data layer - and leverages the companion research project “Optimization of Military and Commercial Goods Movement Through Southern California Using Information Technology” in its regional trade data derived database, and optimization and command and control planning elements. Likewise, supply chain security planning, as described earlier, serves velocity as well as resiliency and recovery objectives as well.

Collectively, these progressive phases will validate the tiered approach embodied in the planning model. Finally, the research team plans to lead and actively support the Interagency Freight Technology Working Group in its “Container of the Future” project as the natural culmination and synthesis of earlier work in supply chain management, goods movement, and trade facilitation, and seaport and supply chain security.

The specific steps necessary recommended by the research team include:

- Map the post 9/11 inspection process flows as the Customs-driven regulatory environment in relation to the end-to-end global supply chain operational context;
- Select complementary inspection technologies for initial evaluation to test the hypothesis of an integrated inspection platform susceptible of deployment in an origin or destination port in a large marine terminal, common high-risk inspection facility, or intermodal rail transfer facility;
- Design a series of graduated laboratory experiments evolving into later field experiments in destination port, designed to develop an integrated inspection platform, independently evaluate operational performance in identifying stimulants and contraband using known sample structure

- techniques for laboratory analysis, and develop specification and performance based standards for operational deployment;
- Develop a data collection plan that incorporated meta-heuristics (neural nets) to teach the technologies to identify contraband from other than known samples, and later in comparison to sample target trade data as well as archived images;
  - Develop and map a relational data layer, based upon goods movement trade data in the form of electronic data interchange messages using standard data sets as the basis for testing the correlation between better data (anomaly) analysis and targeting and the utility of national performance standard of 100% of targeted containers;
  - Integrate data sharing of screening examination and trade data for remote analysis and interpretation in a web encrypted environment among inspection agencies as pre-cursor to introduction and eventual integration with ITDS/ACE providing proof of concept of real time data sharing and remote analysis and interpretation of trade data and non-intrusive screening examination data in a seaport environment;
  - Incorporate end-to-end supply chain security oversight including origin and destination port into demonstration, including container E-seal before and after monitoring, and data sharing using Web-encrypted link, and domestic intermodal container movement using E-Seals or AEI;
  - Develop an overall ontology of the trans-Pacific eastbound trade lane and domestic intermodal movement of international freight and design of collaborative intelligent agents to monitor supply chain security under varying threat levels, recommend corrective actions to reduce risk, modify targeting rules, and adopt measures to mitigate supply chain disruption;
  - Develop an overarching supply chain security strategy based upon risk management principles to measure friction along the supply chain (sourcing, manufacturing, distribution) to quantify and mitigate the impacts of increased supply chain security oversight, develop overall supply chain resiliency through compartmentalization of supply chain disruption and systemic responses, and fostering better individual supply chain agility to avoid/mitigate domestic economic impacts for supply chain disruption and so doing increase deterrence by demonstrating preparedness and response, and reduced vulnerability; and
  - Complete integration (convergence) of supply chain security and velocity components of Strategic Seaport Inspection Process Planning Model through the development, introduction, and deployment of the Container of the Future to provide total asset in transit visibility with on board sensors to minimize probability of intrusion and maximize probability of detection in an operational environment of an agile, resilient, and secure global supply chain and ITDS/ACE with minimum vulnerability and maximum deterrence to intentional disruption.

These steps, combined with the development of a prototype *inspection facility, command and control center and prototype regional rail portal* provide a roadmap for research and, ultimately, deployment of an inspection process that will both improve security and the effectiveness of the supply chain. The Strategic Seaport Inspection Planning Model is consistent with the objectives of the Office of Homeland Security and port authorities and advancing the public/private cooperation necessary to ensure the US security and competitiveness.