

Testimony of
Mr. Rob Quartel

February 26, 2002

I would like to thank the members of this Committee for their invitation today. I'll begin with an assertion that I think should be made policy:

Every container destined to enter or pass through the United States should be treated as a potential weapon of mass destruction; every ship that carries it as a delivery device; and every port and point inland as a potential target.

While the discussion here today focuses on protecting the port -- natural given the legislation before the committee -- the port, frankly, is the least of the problem.

Yes, it's important to protect the security of the physical infrastructure, yes we have to worry about the safety of specialized vessels and guard against attacks like those which took place on the USS Cole, yes, the technology for sealing and tracking containers is important. But in terms of the system of intermodal international trade - shipping, moving goods around the world in international trade - the port of entry is just one - not even the most important - piece of the puzzle.

If you think about trade as a process of integrated pieces, then the port should be considered the point of last - not first - resort in our war on trade terrorism.

To be blunt about it, nothing we have heard discussed today - whether it's electronic seals or port inspections or beefed up patrols or biometric-aided identification cards or GPS or other physical tracking devices on containers or earlier reporting of a ship manifest or neutron scanning 2 percent or 20 percent of all containers going to the United States - whatever -- has more than a small probability of stopping a determined terrorist from slipping a lethal shipment into the mainstream of international commerce and driving it under the Golden Gate Bridge to an end that none of us would like to see.

That's because the action starts well before the port.

So, focusing on stopping a weaponized cargo at the US port is too little, too late: The port is a potential target, not just a gateway. Ports have little interaction with cargoes other than to lift them off or on the ship, to store them, or to serve as a border funnel for customs activities. Their job is in some respects no different than that of a rail yard or similar intermodal exchange node. They are either efficient pass-throughs, propelling cargoes on their way to their final destination - or, they may become bottlenecks, driving some 20 percent of the national economy into the ground.

If we can't allow a weaponized container in a port, neither can we allow it on the ship, the principal means of delivering goods in intercontinental trade to the United States. Ships

suspected to carry these weapons - some ships of which today carry the equivalent of 6500 or more containers -- can only be turned back to the point of embarkation - not stopped, searched, and accessed for removal of an 8x8x48 foot 20-ton container while on the high seas

Interdiction of terrorist activities really needs to begin at the beginning - with the shipper and his customer, at both the physical and transactional start of an order.

While I fully support the measures designed to protect our seaports contained in this legislation, I suggest to this committee that the first line of defense in the future isn't the traditional physical border the port represents, but a new technology border - a virtual, electronic border - that we need to push back overseas.

So, when we talk about technology in this hearing, I think we have to talk about information technology, first - because THAT is the first line of defense for our ports.

The fact of the matter is that we can't inspect every one of the 17,000 containers that end up in the United States on any given day, either here or in the overseas ports in which they originate, without destroying the fabric of our economy. But we CAN create a hierarchical approach combining physical inspection, human trust procedures and a new process of early electronic inspection employing the latest in information technologies.

Why is this electronic border a necessary approach? If I can, let me turn your attention to a couple of slides.

This first slide illustrates a key point: International trade is a tremendously complex business. A typical trade will have as many as 20-25 involved parties - buyers, sellers, inland transporters on both sides of the ocean, ocean and other water carriers, middlemen, financiers, governments and others - and will generate 30-40 documents. Some 6 million containers, many carrying cargoes for multiple owners and valued on average at \$60,000 each, entered the US in the year 2000, on ships carrying from 3-6000 containers each. If we were to add a physical inspection to one of the very large ships carrying these cargoes to the US through the world's hub ports - the Regina Maersk, for example - a single hour's delay per 20-foot container would add from 150 - 250 man-days (roughly 1 ½ to 3 man-years of work shifts) to the time it took to offload the 6000 containers riding that one ship.

Literally millions of people and hundreds of thousands of companies worldwide are engaged in the business of moving cargoes internationally. In the US alone, there are an estimated 400,000 importing and exporting companies, 5,000 licensed forwarders and customs brokers, perhaps as many as 40,000 consolidators large and small, and millions engaged in the transportation industry. Worldwide, there are at least in theory some 500 ocean carriers - although probably 10-15 carry 90 percent of cargoes shipped between continents - an estimated 50-70,000 forwarders and tens of thousands more intermediaries, not to mention several million companies moving goods.

This is a process that literally spews data - data on the contents, on who touched the cargo, who paid for it, where it's been, where it's going.

And it's a process into which commercial shippers - the people who own, buy, or sell a cargo - tap into daily, in one form or another, to collaborate on transportation and financial transactions, to exchange documents, to meet regulatory requirements of the various jurisdictions in which they operate, in addition, of course, to documenting the basic buy-sell transaction that begins the shipment.

So, when I look at what technology you need to protect a US port, I look back to the beginning of the process, before the port, before the ship, before the port of embarkation, before even sealing the container. I look to the buy-sell transaction and the purchase order that is generated from it. Then I look to the manufacturer or supplier overseas, his manufacturing and supplier processes, how and where he or a consolidator somewhere loads the container, when and how it was sealed, how it was moved, who touched it, who paid for it - and even where it might be going once the cargo reaches the United States. For the most part, every bit of that data is available - somewhere and in some form, but not necessarily captured in one place by the private sector, and certainly not by the US government - but there nonetheless, before the cargo ever gets loaded onto a ship bound for a US port.

Throughout this process, the shippers of the goods are for the most part physically out of control of the trade. They've hired freight forwarders or consolidators or third party logistics companies to handle the business because their expertise is in the manufacturing, marketing, and sale of the product. All they really care about at the gross level is that they get exactly what they ordered - no more and no less - and that it gets there at the time and price promised. Some have created intelligent order systems, spent millions of dollars on enterprise resource planning and automated customer service systems, and others have acquired or constructed internally services like those offered by my own company which allow them to track, measure, and steer the progress of their goods through the transportation chain, either physically or in terms of process and paperwork, the latter actually being more important in the manufacturing process than where something actually is. As long as they know it's on course, are apprised of delays, have the ability to re-plan a move or a manufacturing process in the event of a supply chain problem - than they are satisfied. That's really all they need.

The focus of logisticians and companies - particularly American companies - over the last several decades has been on making that flow faster, cheaper, more transparent, and faster yet. Our success at that provides an enormous competitive advantage to many of our companies and makes a huge contribution to the reduction in the cost of numerous articles and products crucial to everyday life in the United States.

Some in the government have suggested that, as in aviation, security rather than speed might provide the competitive edge for ports in the US in the future.

With all due respect, speed and cost were the two most important criteria for the selection of ports and transportation before September 11 - and they will, for all but a handful of shippers - continue to be the most important criteria in the future.

There is a reason for that: Speed equals money.

Because the manufacturing system knows that, logistics costs have steadily declined from 25 percent to lower than 15 percent of GDP over the last 20 years. Carrying costs associated just with inventory at rest - goods in storage, the response of a manufacturer to uncertainties in the supply chain - in 2000 amounted to nearly \$400 billion. A number of experts have estimated that just a five percent addition to the logistics process - thus causing an increase in inventories, the response industry will have to take in order to make up for slow processing times - would cost the economy an additional \$75 billion annually. That's the equivalent, by the way, of some 75,000 jobs lost, not counting the multiplier effect of these wholly non-productive costs

Introducing uncertainty, slowing down cargoes through physical inspection of every container and every box inside it, otherwise derailing the transportation system, is exactly the opposite of what we should do if our goal is to maintain a healthy American economy.

So, the most critical piece of the technology solution to guarding our ports, in my mind, is this: Profile cargoes, just as we profile people in the passenger airline industry, before they ever get on the ship - or plane, truck, or train - bound for the United States and its ports.

The data that the private sector uses to make its processes more efficient is the same data that the United States government needs to understand the commercial processes underlying a cargo profiling process.

My second slide talks to that process, but in short form, it's pretty straightforward.

In the profiling scheme that I have suggested, commercial data would: (1) Be captured prior to loading of a container on a ship, train, plane, or truck in international commerce, from the shipper, consignee, intermediary, banks, and all others that had an interest in or touched or processed the shipment; (2) Combined with certain relevant law enforcement and national security information; and, (3) Be processed through a form of artificial intelligence (including evolutionary computing) to provide a "profile" for every container and shipment within it. The profiling process would generate a "go-no go" decision driving further actions - loading on a carrier, physical inspection, further profiling, etc.

The profile would be based not only on what the cargo was said to be, but where it came from, its likelihood of being what it is stated to be, who handled it from packing through transport to a port, who would be handling it afterwards, where it had been and where it was going, who had a financial interest in it, etc. The algorithm would need to consider not only fact-based data (eg, what the product was and who touched it), but situational data - eg, a container originating in an unstable country and passing by Yankee Stadium on the day and hour the President was scheduled to throw out the first ball.

Based on some probability calculus, the air, ocean, train, or truck carrier could be told that the government either felt the cargo was safe to carry - or - that further investigation, including perhaps a physical inspection, was necessary. If a carrier then loaded the cargo deemed safe and was later told enroute that the cargo might require further investigation, then the carrier - having cooperated with the USG on the pre-release process - should be held harmless from further government sanctions, although it might well have to divert the vessel prior to or on arrival in a

US port. (Indemnification here is a form of positive coercion that avoids the extraterritoriality issue.)

If a carrier received notification that a shipment was suspect prior to loading, it should then be required to arrange to have the cargo physically screened, or disclose why not. Screening could be carried out by U.S. Customs officials stationed in overseas points, foreign officials subject to bilaterals and some level of performance auditing, or by the companies themselves, again subject to performance auditing and rigorous procedural standards. The actual inspection could take several forms, ranging from passively examining the container (neutron scanning, motion detection, etc), to employing radiological and chemical "sniffers," to breaking the seal and opening it up.

Each of these methods has costs, risks, and probabilities associated with it and would be employed differentially against the perceived calculated risk. Screening might, in many cases, consist merely of re-checking documentation for inconsistencies and communicating with those who provided the documents to clarify the issue. Breaking a seal would, however, require some form of indemnifying the carrier, including possibly an entry order to do so from US Customs. None of these actions, however, have to involve a foreign government. The United States has the authority to deny entry of vessels that it deems of risk to itself, and to deny entry of goods deemed illegal. Providing process incentives to carry out the inspection prior to leading the port or embarkation is a legitimate, effective form of positive coercion. In the end, however, there is no doubt that the support of foreign trading partners and international organizations should be solicited, if only because our leading trading partners are themselves potential targets and will no doubt feel the need for reciprocal protections.

This raises other issues, of course, one being the question of whether or not we would need to place US Customs inspectors inside foreign ports of embarkation. My answer is: Maybe yes, maybe no. US government agencies frequently place inspectors, expeditors, and agents inside the premises of companies in the continental United States, sometimes with and sometimes without the invitation of the private companies involved. Companies often place employees whose job it is to ascertain quality, manage logistics, and to perform other expediting services in the home facilities of suppliers or customers, again at the invitation of the parties. US Customs inspectors could certainly be stationed inside the facilities of major carriers and manufacturers overseas, at their invitation, without generating an official response from a foreign government, in order to provide processing capabilities. Carriers and manufacturers that did this - whether by invitation or by USG mandate - could legitimately be considered "trusted parties" and receive "fast lane" treatment on arrival in Customs in the United States, assuming that proper cargo security procedures were employed across the length of the supply chain.

The bottom line, however, is that this is NOT about inspecting the majority of containers or shipments. The goal, in fact, is to use information technology to substantially reduce the need to physically inspect containers, and to do so at a point in the logistics process that is the least damaging to it economically, and at which diversion of a contaminated cargo can be safely accomplished without delaying other cargoes.

Nor, by the way, is this about enforcing US customs compliance rules overseas - something that frequently seems to be mistaken for the prevention of terrorism in many of the proposals placed

on the table. This is about determining which cargoes might be a threat to the United States and its citizens, not about whether or not US tariff rules are complied with. The latter has only a little to do with helping to ascertain the former, which is largely a function designed for revenue capture. Not only are these not the same things, but, treating this process as a means of enforcing customs rules could actually undermine the anti-terrorism effort. A legal cargo can become a lethal cargo under the proper circumstances. Thus, treating this as a customs compliance problem not only doesn't solve the problem, it actually lulls the public and the USG into a dangerously false sense of security.

There are three important attributes to this solution and the approach I suggest. First and foremost, it taps into the existing commercial trade management process and leverages existing relationships into a new holistic structure. Second, it is potentially fully independent of the need for international cooperation, as it requires only the compliance of the US-side of the equation, particularly if process compliance was specifically designated to be the responsibility of the buyer, a suggestion I have made elsewhere. And, finally, it is an approach that makes the greatest use of the technologies being developed by the private sector for use by commercial customers in a normal but obviously complex operating environment.

All of this is easy to suggest, of course, and somewhat more difficult to implement.

But, to give you an idea of where we actually stand, four existing commercial documents already reported in one form or another to Customs and the Coast Guard can provide much - but not all - of the data that would allow us to profile a cargo based on contents, involved parties, and transport mode and path prior to its ever getting on a ship: (1) The Shippers Letter of Instruction; (2) Commercial Invoice; (3) Certificate of Origin; and (4) The carrier's Bill of Lading. To that I would add (5) financial data, perhaps captured through Letters of Credit or bank reporting; (6) Inland transportation leg information not now captured by ocean carriers or the government, on both sides of the supply chain; and perhaps additional information.

On the commercial side, database structures already exist that are designed to integrate data from disparate sources (for example, EDI transmissions, faxes, the web, and email) and that, in computer parlance, allow you to instantiate a fully attributed shipment. Why a shipment? Because trade moves in shipments, first, and only then in containers. From the standpoint of profiling, shipment records need to be fully attributed - meaning that they need to contain detailed information about the shipment including all of the parties that are involved in the transaction, the route/itinerary of the shipment, the items that are contained in the shipment, the events/status of the shipment and its financial terms and any other information that was thought necessary. And, the system needs to be able to collect, process and integrate this data and to provide the required normalized data elements to support container and risk profiling in support of Homeland Security.

Collecting and managing the commercial data isn't rocket science, although not a lot of us do it. But it is what the private sector is beginning to look for today.

Analyzing the data IS rocket science, however. But, again, the required processes are already in use inside the government and the commercial sectors alike - in everything from looking for illicit drug traffic to screening genetic samples for new drugs for medical purposes.

Without going into a lot of detail, the analytical process should be designed at the simplest level to check against lists - Denied Party Screening, for example; and at the most complex level to think, to learn, and to detect deviations from what we know in our own experience is normal in the operations of international transportation and manufacturing -- anomalies captured in rules and facts which may pertain to both specific and general information, relationships between data, expectations and other expertise. Items that violate expectations or otherwise contradict human expertise are considered to be more suspicious.

But, of course, cargo profiling is only part of the solution. As should be evident from the above description, this is an onion, with numerous layers. At varying stages across the process we have to layer on passive and physical inspection, physical protection of the ports, protection of the cargo integrity from the basic risks of international transport - spoilage, tampering, theft - the ability to interdict specific cargoes, tracking and visibility solutions, many of which we have heard about today -- that allow us to maintain not only the integrity of the cargo but of the transport system itself once a cargo is in motion.

Cargo profiling is an approach and a system that I believe that the Transportation Security Administration at the US Department of Transportation already has the authority to implement - a question separate from whether or not they have the dollars to do so. (I would note that profiling would certainly cost far less and take less time to implement than a full system of inspections, electronic seals, etc.) TSA needs the support, almost in a sub-contracting role, of the US Customs Service, the US Coast Guard, the various modal agencies, and, perhaps the US Department of Commerce alike. The data base process could perhaps ultimately be embedded into and as an extension of the Automated Customs Enforcement (ACE) system that Customs is currently building - but which is scheduled to take another five years to deliver. The US Coast Guard and other national security and defense agencies also have extensive law enforcement and national security data base efforts going on, and numerous government data bases could be tapped through the new process for relevant data without violating the need to maintain the competitive position of individual companies and due process for the parties involved.

I don't believe, however, that we should or need to wait that long to implement a robust, commercially relevant, profiling solution. We should be looking - today -- at other USG data bases, including the so-called ITDS system being developed several years ago at Treasury, outside of Customs, as a possible stopgap; and, we should be looking to the private sector as well for information technology accelerators. Several groups of commercial and governmental players have suggested demonstration projects that would cover ports and inland movements on both sides of the traffic on both the East and West Coasts, using commercially available information technologies and real-world data and cargo movements.

As a general comment here, I believe strongly that a critical issue here will be to obtain voluntary - not just mandatory - commercial compliance with all of the parties in the commercial transaction. Many of the processes covered here are outside the domain of US law enforcement. We can't today make foreign suppliers abide by all of these rules, but we can certainly tell their US customers - today -- that they may face delays unless they know their sources and can validate cargo and process integrity. We can't today tell a foreign port that it has to purchase millions of dollars worth of screening devices for the cargoes destined for the US which our

screening picks out as suspect, but we can - today -- certainly negotiate procedural agreements through the IMO and individual American ports and distribution arms can provide speed incentives for those that work with us. The ocean carriers barely make 1-2 percent ROI, so they will only be driven into bankruptcy if we require that they purchase screening machines and add hundreds of new security personnel, but we may be able to help them through the imposition of a user charge on all cargoes going through US ports, a portion of which is used to offset their additional costs. We can't today mandate that the carriers for which the US is only one of several stops profile all of their cargoes before sailing; but we can no doubt - today -- find a way to say that if we determine that a cargo is found to be suspect the entire ship will be turned back because we won't risk the US port.

In closing, I'd like to reiterate the point with which I began: US ports aren't the first line of defense but almost the last.

This Committee and this government have a real obligation to see that no weaponized container ever makes it to the port, period. They have an obligation to protect the integrity of cargoes once entered, and they have an obligation to their customers - the failure of which to provide will destroy their commercial viability and that of the general economy - to provide a speedy, low-cost transportation move. I believe we have the technical means to tap into the commercial process, to profile shipments and containers, and thus, in concert with other actions, to see that no container intended to be used as a terrorist device ever gets on a ship, a plane, a truck or a train bound for the United States. We have the technology to do it, but the process starts well before a container ever reaches a port.

Members of this Committee: When the aviation system went down on September 11, we already had a security system, as imperfect as it was, in place, which could be re-booted three days later at a higher state of readiness.

However -- If a container blew at a port or somewhere else in the international transportation chain ending in the United States, this nation and its leaders would have no choice but to shut down the entire system of trade with our country. We have no security system in place in our international trade system comparable to that which pre-existed in passenger airline travel that we can re-boot. We have nothing at all in place to properly secure over \$2 trillion in trade and the millions of American jobs associated with it. Electronic seals, tracking, additional port security - none of that will solve that problem adequately. We DO have the technology available to begin to profile shipments aimed at the United States, today. It's not the complete solution, but it's an appropriate start.

Again, I appreciate the Committee's time, and would be glad to discuss it further.

SEVEN THINGS WE COULD BE DOING NOW TO PROTECT OUR PORTS:

1. We should begin the process of moving to pre-movement data filing on the entire shipment process, including not only customs compliance filings, but transportation and financial data. And, we should begin immediately to tighten the document process. Mandating reporting of a manifest four days out is only marginally useful. Better would be to mandate filing of all ship

manifests for vessels with cargoes bound for the US at least 24 hours prior to embarkation from a foreign port, even if only in incomplete form, with confirmation at final departure. The reality of the ship manifest is that it is useful only to document what is believed was loaded on a ship or plane, as a chain of custody certification. Over half of what moves on ships moves "FAK" (Freight All Kinds), meaning that the carrier has no idea what is in the containers it carries. Of the remaining manifest data, at least half is likely to contain inaccuracies. Nevertheless, requiring pre-departure filing of a ship manifest will have a certain "Hawthorne Effect" on the process, meaning that paying more attention to it would induce behavioral changes in the process - ranging from fostering mistakes by individuals attempting to circumvent the process, to exposing inconsistencies in data filings, to reducing errors among those attempting to comply legally because of the presumed additional scrutiny by government officials.

2. Shippers or consignees or their agents should be made legally responsible for complying with all data mandates on a timely basis. We should consider the immediate implementation of a purchase-order entry system, in which individuals purchasing goods from overseas should file a notification of the purchase and expected entry date and related parties early in the process; and they should perhaps in return be given an import number against which all subsequent data and documentation is filed. This is not a suggestion for an Import License, which would require a new bureaucracy, but simply the assignment of a number for later data and cargo tracking.

3. We should make better use of intermediaries in the international trade process. Over 80 percent of all cargoes in international trade are outsourced in whole or in part to freight forwarders, customs brokers, NVO's, consolidators, 3PL's and other who are expert in the process. Most of these parties are already licensed by the US Federal Maritime Commission; and their numbers are small (4000 forwarders, for example), so their activities could be monitored. Licensing procedures should be intensified, perhaps including the addition of background checks; and the licensing and oversight of these regulated entities moved to the US Customs Service where there are more and better resources for this activity. Forwarders and other licensed entities should be enlisted today, and issued a set of procedural scrutinizes NOW that would allow them to become part of the "watch" process.

4. The US should consider adopting and mandating the use of the International Bill of Lading owned by the International Freight Forwarders Association (FIATA) as a means of introducing consistency into cargo documentation.

5. We should mandate conversion to electronic data transmission (whether by EDI, web, etc) from all modes and players in the transportation and trade process by a date certain.

6. The Transportation Security Administration in DOT should formally, publicly be placed in charge of the profiling and international trade process. Transportation is the one constant in an international movement. The USCG, Customs, and the Office of Naval Intelligence should be enlisted as "sub-contractors" for various parts of the program. The US Department of Commerce should be considered as the point at which the PO Entry System is filed, and the place from which a "go-no go" decision is conveyed from the USG to a commercial carrier.

7. We should begin immediately to test implementation of a container profiling process that originates overseas, using commercially available data base structures, algorithms, and

knowledge. The data issues contained in aggregating information on a cargo, its movements, the players that touch it, across multiple modes and legs, and transmitted by the variety of electronic and non-electronic means, have already been solved in large part by the private sector seeking to obtain transportation and supply chain visibility and control.