DAY 2: CONCURRENT PANEL SESSIONS (PANEL 1B)

Cargo Clearance, Security, and Safety

Robert North, *Rear Admiral, U.S. Coast Guard, Moderator*
Alan Spear, *Intercargo Insurance Company*
Stephen Flynn, *Commander, U.S. Coast Guard Academy*
John McGowan, *U.S. Customs Service, Interagency Commission on Crime and Security in U.S. Seaports*
Jeff Black, *Micronpc.com, Technology Asset Protection Association*

OVERVIEW

Rear Admiral Robert North

Our focus today will be issues such as border and port of entry clearance, international equipment and safety standards, efficient transfer of goods, cargo, liability, cargo crime, and security issues arising from a number of factors, certainly including more traffic congestion, multiple users of the transportation system, and the intermodal aspect of what we do out there.

Cargo security certainly is not a new issue, but it is a particularly topical issue to talk about today. It is being addressed by the Interagency Commission on Seaport Crime and Security, which has held listening sessions around the country. Safety and security are both issues on the agenda of U.S. Secretary of Transportation Rodney Slater and a host of stakeholders as part of the U.S. Department of Transportation Marine Transportation System initiative. The panelists have extensive knowledge, expertise, and experience with cargo safety and security issues.

CARGO CRIMES INVESTIGATION

Alan Spear

Alan Spear is Director of Loss Control at Intercargo Insurance Company. Not only has he developed and directed Operation Intercept, which has recovered nearly 30 percent of reported stolen cargo, but he is also a former Coast Guardsman.

Cape May is at the southern tip of New Jersey. It is a resort community. The Coast Guard boot camp at Cape May is built on a World War II airfield. It is not a resort community. As a seaman recruit at Cape May in December 1965, I am sure I was wondering if I would ever be introduced at a prestigious national conference by a Coast Guard Admiral. At the time, it was five below zero and blowing 20 knots, and a Chief Boatswain's Mate was yelling at me—times are better now. In all seriousness, thank you for the introduction and I am truly honored to be here and to have been introduced by Admiral North. Unfortunately, I do not bring you a happy message.

I work for XL Specialty Insurance Company (Intercargo), which insures cargo, and I run a cargo crimes investigations program called Operation Intercept. In 3 years, that program has recovered $4,300,000 in stolen cargo, but it has investigated nearly $17,000,000 in losses. Cargo crime is epidemic in this country. Fifty percent of our inland and ocean marine losses in the past 2 years were the result of cargo crime of one type or another. It is my perception that cargo crime may be as bad or worse in some parts of this country as it is in almost any other country in the world.

Throughout recorded history, cargo has been moved from point to point and placed in storage, and thieves have stolen it. Bandits, highwaymen, and pirates beset early cargo carriers, and when Lloyd's of London was formed

in the 1600s, one of the recognized perils of transit was cargo theft in all its variations. As the technology changed, so changed cargo theft. When we used wagons, they stole cargo from the wagons or they stole the wagons. When we used ships, they pirated the ships and stole the cargo, sometimes stealing or sinking the ships. Early rail was beset with robbers, much like those who still climb aboard slow freights near the U.S.–Mexico border, but the overall character of cargo crime changed dramatically during the past 10 years, building on events that occurred in the 1950s and since 1985. In the 1950s, we invented the intermodal system, and in the 1980s we invented practical personal computers. Together, these inventions changed the face of cargo crime in the decade of the 1990s and beyond.

In a cynical sense, the current state of cargo crime is indirectly the fault of two famous and respected Americans: Dwight Eisenhower and Malcolm McLean. Eisenhower was the driving force behind the creation of the Interstate highway system, which he thought was necessary to ensure the efficient movement of troops and materials to all parts of the continental United States in order to be able to best resist an invading army. The creation of that highway system made it possible for interstate trucking to compete effectively with the railroads and opened the door for another innovator, Malcolm McLean. In the mid-1950s, when McLean first drove a truck aboard a ship in New Jersey and took it to Texas by sea, intermodalism was born. The concept of moving cargo by different modalities within the same box or trailer became viable. The incredible efficiency and speed of the intermodal system has not only opened the door to intermodal world commerce, it has also provided great opportunities for cargo criminals. Further, the sudden practicality and popularity of computers and high-value consumer electronics made it common to ship loads of cargo worth well over a million dollars in containers. Price increases on cigarettes raised the value of a container of smokes from $100,000 to over a million dollars. With ample targets as a result of the booming economy, and plenty of ammunition, cargo criminals have been having a turkey shoot.

Two primary characteristics of the intermodal system have changed the face of cargo crime. The first is that the system is so efficient that stolen cargo can now be moved extremely rapidly around the world. A load stolen in California can be exported from New York within a week, or it can cross the border into Mexico within 12 hours. Freight forwarders, who often see only the paperwork, are used, generally without their knowledge, to move stolen cargo through legitimate cargo transportation systems. Given the incredible volume of cargo on the move, and the limited resources available to the U.S. Customs Service, most cargo moves in and out of this country without ever being checked once the doors are closed and seals are applied.

The second characteristic, which also serves to prevent certain kinds of theft, such as pilferage, is the innocuous character of containers. Without the paperwork, there is no way to tell what is inside. If the cargo is stolen computers, and the paperwork says miscellaneous furniture, it will likely be treated as miscellaneous furniture throughout transit and may well exit the country with that designation. On the other hand, the innocuous character of containers should prevent theft because cargo thieves should not be able to tell which container holds valuable cargo and which does not. This being entirely true, one would expect cargo to be stolen in proportion to its frequency. In essence, we should have more theft of foodstuffs than anything else because there are more containers holding food than there are holding computers. Our statistics show, however, that of the $10,000,000 in investigations we conducted last year, $4,172,600 were for computers and consumer electronics (24 claims) and $300,500 were for foodstuffs (six claims). These data suggest that most high-cost thefts occur because of inside information. I guess this means we can blame Eisenhower, McLean, and insider information.

Unfortunately, the fault lies also with the participants in the intermodal system, primarily as a result of the common practice of passing the buck. Shippers play their part when they pass the buck to truckers (if it gets stolen, the trucker will pay the loss). Truckers play their part when they pass the buck to underwriters (it's insured). Underwriters pass the buck when they repeatedly underwrite bad risks (maybe it will get better this time), and, in the long run, consumers pay the price and criminals get the bucks. By refusing to implement good security practices, even the most elementary efforts to protect cargo in storage and transit, shippers, carriers, and underwriters are subsidizing the cargo theft industry. This frequent refusal to accept responsibility leaves the door open to thieves. Shippers who mark their boxes so that thieves know they are valuable (does anybody here not know what is in a box with "cow" markings?), carriers who park valuable loads in abandoned K-Mart parking lots, underwriters who place premium ahead of prevention, government that inadequately supports law enforcement efforts to fight cargo crime, and law enforcement that embroils itself in turf issues and is frequently uneducated about cargo crime yield a pattern of inadequate response to the problem that ensures that cargo crime will not only continue, it will worsen in the decades ahead.

Four things need to happen to give us any chance of winning this war:

1. First, and foremost, we must provide additional support for law enforcement cargo crime task forces in all our major cities. Tomcats in Miami has 21 full-time officers and is so overworked they cannot provide a full investigation for any loss under $200,000. Los Angeles has

at least four cargo crimes task forces: Cargo Cats, Bad Cats, the FBI, and CTIPS, and they are all overworked, notwithstanding the ongoing divisions and political issues that make their jobs more difficult. Chicago is politically immobilized and has no real multidisciplinary task force. Memphis has its act together and supports an outstanding task force, Atlanta has nothing at all, and the Columbus, Ohio, police department, in one of the primary transshipping locations in the country, thinks cargo crime is the same as automobile theft.

2. Second, insurance companies, shippers, carriers, and law enforcement must join together to share information, much as they do through the National Insurance Crime Bureau. That particular group is too bureaucratic and single-visioned for this job and has no focus on cargo crime, but a group must be found, or a new one created, to combine and compile information on cargo crime that is accessible to law enforcement, investigators, shippers, carriers, and insurance companies. Current efforts, like Cargo Tips at the American Trucking Associations, are noteworthy, but they leave out some of the key players and are not interactive enough to serve as investigative tools. Understand this—we have been talking about $10 billion in cargo crime in the United States annually for about 5 years now, yet that figure is unsupported by any hard data. We really do not have a clue about the financial impact, either directly or indirectly, and that is the least of the problems. Police in Texas recently found five stolen loads in a warehouse. They spent 6 months trying to find the owners and underwriters of the cargo, but, without a central database, finally gave up and sold the cargo at auction. A load of batteries went begging in Chicago, and although a load of computers was partially recovered in Los Angeles, it was recovered only because an insurance company personally notified Cargo Cats of the loss. Salt Lake City Police had the loss recorded as automobile theft.

3. Third, cargo crime must be more strongly criminalized by statute. Organized crime is shifting resources to cargo crime because it is easy and because the penalties are minimal or inconsistent. Neither state nor federal courts are consistent in their handling of cargo crime, and the options available to those courts that do pay attention are too limited.

4. Finally, we have to stop passing the buck. Truckers who do not follow good security practices should not be insured. Shippers who are careless about how they hire personnel, how they protect information, and how they choose carriers should feel the pain of cargo crime instead of dumping it on somebody else, and underwriters need to wake up and realize they cannot allow the drive for more premiums to overwhelm the requirements of proper security and loss prevention.

I can tell you this right now: small drayage carriers in the Los Angeles–Long Beach market are not insurable for cargo theft at any kind of reasonable rate. The same is true in Miami, and it is becoming true in New Jersey and New York. Without extraordinary security precautions, valuable cargo cannot be reasonably insured against theft in most of South America, most of Central America, any of the former Soviet republics, much of Africa, and parts of the Far East. Computers and consumer electronics, tobacco products, and other high-value cargoes are rapidly becoming potentially nonviable as insurable risks because of both the concentration of value in each shipment and the risk of theft. The cargo crime situation in this country is grim and truly out of hand in some cities here and in many overseas.

I am going to shift to an entirely different picture—still cargo crime, but a different type of cargo crime. This is a true story, it is still happening, and it gives a real sense of the global implications of cargo crime and some of the incredible complexities of dealing with it. This crime is called barratry, an old English term meaning the illegal seizure or theft of cargo by the master and crew of a vessel.

In June 1999, a U.S. Coast Guard law enforcement detachment, working in cooperation with the British Navy, arrested the vessel *China Breeze* off the coast of Puerto Rico. She was carrying 8,800 lb of cocaine, and her arrest turned out to be the eleventh largest maritime cocaine bust in history. She was registered in Panama and shown as owned by Moccha Marine Ltd. Lloyd's List (January 26, 2000) states that she was in fact owned by an individual, Elias Kellis, who is now reportedly in jail, and was the same person who owned a vessel called *Kobe Queen* through a Greek company called Nominator. The prior master of *China Breeze*, although not at the time of her arrest, was a man named Yuri Livkovsky. He later became master of *Kobe Queen I*. He was not connected to the drug smuggling charges placed against *China Breeze*.

The story now moves to *Kobe Queen*. At about the same time, in May 1999, five steel brokers in Europe and the United States chartered the *Kobe Queen* through a chartering broker called Reliant, a Greek company. Chartering means that each of the brokers contracted for a percentage of the vessel's capacity, and Reliant made the arrangements on their behalf. Under the chartering agreement, *Kobe Queen* was ordered to pick up steel and chemical cargo in Turkey, to make a stop in Greece, and then to proceed on to Dakar, Senegal, to discharge the chemicals. The steel was destined for three ports in the Caribbean. With her owner in jail, *Kobe Queen* was being managed by a Ukrainian company named Babush. We theorize that Babush, knowing that the sister ship, *China Breeze*, had been arrested, and that the owner of both ships was Greek, determined to order the vessel to bypass the assigned Greek port in order to avoid possible arrest, and then ordered the *Kobe Queen* to proceed

directly to Dakar, where she discharged 2,100 million tons of chemicals on August 3, 1999. Radiant, realizing that *Kobe Queen* had broken her charter agreement and failed to stop in Greece, withheld $123,000 (U.S. dollars) from its payments to Babush. In retaliation, Babush ordered the vessel to stop about 200 mi off the coast of Dakar near the Cape Verde Islands. At about that time, American P&I Insurance Company canceled insurance on the vessel because it had questions about the possible connection between the ownership of *China Breeze* and *Kobe Queen* and their inability to get Babush to answer questions about the matter. The vessel was drifting, and uninsured, with cargo on board.

Late in August, we were notified that the steel cargo we had insured on the vessel had not been delivered to consignees in the Caribbean. It was rumored at the time that the vessel had been seized by Senegal authorities on suspicions of smuggling drugs, but this turned out to be a misinterpretation of the experiences of her sister ship, *China Breeze*.

After some research, we discovered some of the actual circumstances and sent Jurgen Schulze of the firm of John Alder and Associates of New Jersey, to Istanbul, Turkey, to negotiate with Radiant and Babush in an attempt to get the cargo moved forward. On September 5, Babush told Jurgen the vessel had been drifting for a month and was out of food and bunkers and needed to be supplied. They demanded not only the $123,000, but an additional $80,000 for supplies. Jurgen worked through two marathon sessions and obtained a memorandum of agreement whereby cargo interests, whoever they were, would pay $123,000 when the vessel arrived in port in the Caribbean and $80,000 once the cargo was discharged. Babush demanded that cargo interests also agree not to arrest the vessel and further demanded original letters from every cargo interest, on their letterhead, confirming the terms of the agreement. At this point, we did not know who else had cargo aboard. We found the terms distasteful, especially because cargo interests really did not owe anybody anything, but Radiant had backed out entirely and we had over a million dollars at stake.

Jurgen returned to the United States and began to research the other cargo owners and insurers, finding that Fireman's Fund, AGF/MAT of Belgium, and a Breffe & Henke of Germany company also had cargo insured aboard. We later discovered that two Dominican insurance companies had also insured cargo on the vessel. Until this point, Intercargo had remained in the background, not wanting Babush to know that an insurance company was involved. Jurgen had passed himself off as representing our client, Global Steel, and continued to do so while he contacted and arranged the support of the other steel companies and insurance companies with cargo aboard the vessel.

In late September, we discovered that Babush had lied, and that the vessel had bunkered and received food from a barge off of St. Charles Cape Verde Islands on September 3, 2 days before Babush told us the vessel desperately needed supplies. Attempts to address this issue with Babush failed.

Throughout September and October, we continued to try to negotiate with Babush. Every morning we read voluminous e-mails on our home computers, spent the trip in to work on the cell phone discussing the matter, and spent 3 to 4 hours every day working the case. It became all-consuming. During the course of this investigation, over 1,000 e-mails were sent to and from Intercargo alone. Figuring in the other parties, over 12,000 e-mails were sent. We had communications translated into Ukrainian, we sent FedEx packages, we sent telexes to the ship (confirming her general location by the location of the satellite receiving her responses), and we retained an international investigative firm to research the people involved and the issues. Among a great deal of useless information, the firm told us the vessel was suspected of drug smuggling, that the owner was in jail, and that Babush were bad people—Russian mafia, they said. In October, another party, Crescent Marine, was retained by Babush to negotiate on their behalf but they eventually discovered they could not trust Babush and withdrew—we had spent hours working with them on the matter. By late October, all the cargo interests, except the Dominicans, were working together, with Intercargo using John Alder and Fireman's Fund using MRC in London. We tried to keep everybody informed and on board and the copy list on e-mails extended more than a page.

We discussed the problem with a number of steel brokers and determined that if Babush and the crew wanted to sell the cargo illegally, they would likely have to go to a semilegal port where they could bribe port officials into allowing the cargo to be sold illegally. No legitimate port would allow sale of the cargo, nor would it allow the ship to berth without Hull P & I insurance because the ship was not covered for any sort of liability, such as oil spills or sinking in midchannel. The nearest likely place, with any sort of market, was Lagos, Nigeria. In early November, we notified all the Lloyd's surveyors in Africa, South America, Europe, and the Caribbean that the vessel was wanted. On November 18, we were contacted by Lloyd's agents in Lagos, who advised us that the ship was anchored outside of the harbor and was requesting docking space to discharge cargo. I got this news on the cell phone while I was driving to work and nearly drove off the road. We were yelling and shouting, "We got it, we got it!!" We immediately retained counsel in Lagos, and, by heroic efforts and a judicious use of funds, counsel was able to generate an arrest warrant from the Lagos courts in 24 hours. Then we had to wait—nobody would take a boat out to

the ship because the incidence of piracy is so bad in Lagos that anyone approaching a ship in a small craft is likely to be shot. Two days later, we were advised that the ship had bunkered from a barge, purchased supplies and charts, and left the port area. Through the use of more funds, the Lloyd's agents were able to obtain copies of receipts for fuel, food, and charts purchased by the ship and found that she had bunkered 680 tons of diesel fuel and enough food and water for 30 days. She had also purchased charts for South Africa, the Mozambique Channel, Madagascar, the Red Sea, and the Persian Gulf. At this point, we realized the game was up and Babush had no intention of allowing the vessel to proceed to the Caribbean, so we took more drastic action.

Intercargo went public and identified itself and its role to the other cargo insurers. Working with three other insurers, we offered a reward of $100,000 for anyone providing us with information leading to the arrest of the vessel and recovery of the cargo. By this time, we knew the full value of the cargo aboard was $4,500,000, of which we had insured about 22.3 percent. We contacted the vessel master and offered him the reward if he would return the vessel to the Caribbean. We offered to provide funds for his family and to fly the crew home from any port to which he would take the vessel. At the same time, we attempted to obtain help from Interpol and the U.S. State Department without any luck whatsoever. German police were also contacted, without result. We met with the FBI, and talked with the U.S. Drug Enforcement Administration and got nowhere. The master refused to cooperate, telling us he took orders only from Babush. We reminded him he had bills of lading directing the cargo to the Caribbean, and he told us he had to take orders. In desperation, we told him that if he did not cooperate, we would declare his vessel criminal through the world press and would ask the Ukrainian government to withdraw his license. In response, he shut down his telex system entirely and refused to respond in any way to communications. According to AT&T, his last telex communication came from the South Atlantic.

Meanwhile, Babush disappeared also. We sent investigators to their offices in Odessa and were told by neighbors that they were bad people. We checked the homes of their owners and found them empty; we attempted to trace their corporate records and found none. We checked registry and licensure records in Greece, the Ukraine, and Cypress and found no record of any company named Babush. We found the home of the captain and interviewed his wife and parents and were told he was due home in late December, but they were unable or unwilling to tell us where he was. We filed complaints with the Ukrainian Maritime Ministry, and we attempted to trace bank accounts and funds back to Babush and its owners. We found that the funds used to buy the fuel in Lagos came through a British intermediary, and we had investigators in London visit them. They were convinced not to cooperate with Babush in the future, but none of these efforts succeeded in flushing out *Kobe Queen*.

Suspecting that the ship was bound for the Indian Ocean, we figured Babush intended to try to sell the ship and cargo to ship breakers in India or Bangladesh and that they might try to do so under a different vessel name. Ship breakers are kind of like the elephant graveyard for ships. Old vessels are brought in close to shore at the highest tides of the month and driven ashore at maximum speed on mud flats or sand bars. Once the tide goes out, hundreds of people descend on the vessel and cut it to pieces, and after a few months, nothing is left. The parts of the vessel are sold in salvage or as scrap. In Alang, India, there are over 100 ship breakers; there are more in Karachi, Pakistan, and Bangladesh. Knowing this, we notified every Lloyd's agent and port authority in Pakistan, India, and Bangladesh that the ship was wanted. We heard nothing for over 40 days. Finally, four of the insurance companies paid their claims, leaving the status of 29 percent of the cargo, which was insured by Dominican insurance companies, uncertain.

On December 24, 1999, the *Kobe Queen*, renamed the *Gloria Kopp*, was arrested by the Indian Coast Guard about 13 mi offshore from Pondicherry, India, 30 mi south of Madras (which is now called Chennai). The vessel attempted to escape, and the crew was taken at gunpoint. The vessel was then towed to Chennai. On December 25, at 2 p.m., as we were sitting down for Christmas dinner, I received a call from a representative of the Fireman's Fund, telling me that when the ship was taken by the Coast Guard, Captain Livkovsky had hanged himself in his cabin, leaving a note that he felt abandoned by Babush. We knew the captain had a wife and children and all of us involved were affected by the news.

First notification of the find had come from Wilson and Company, Lloyd's surveyors in Chennai, who claimed the $100,000 reward. Almost immediately, other claims against us and the vessel began to pour in. The Coast Guard demanded the reward and other unspecified amounts. The port authority demanded funds, Wilson sent us a bill for $28,000 for nothing specific; people who had looked for the ship but not found it sent us bills for their time. Seeing that the situation was getting out of hand, we sent a representative to Chennai to represent the four cargo interests who had participated in the search. He spent two agonizing weeks trying to get cooperation from anyone. He found that the crew had convinced the Coast Guard that the entire problem was the fault of cargo interests. The Coast Guard had

14 men with AK47s on the ship guarding the crew and was demanding that we feed and supply them. Four other Indian government agencies—drug enforcement, customs, immigration, and the port authority—were involved.

We hired counsel and went to court to obtain formal arrest of the vessel and cargo and to request permission to bring the ship to shore to discharge the cargo into another vessel. At this point, it was discovered that the vessel's main engine had cracked two cylinder heads from being operated with salt water cooling and that one of her two generators was also dysfunctional. As a result, the vessel was no longer self-powered and her offloading gear could not be used. Further, the port was really not capable of discharging the cargo, and the port authority went into court and got an order banning the vessel from entering the port, because she had no power and no Hull P & I insurance.

We had an arrested ship, sitting 6 mi (9.7 km) out in the harbor, with a crew aboard who had not been ashore in 8 months, no main engine, intermittent power, and guys with guns on the decks. Meanwhile, Babush stayed missing, and although the new owner was identified in the ship's papers, he never showed up and never presented anything to the court. For a week, our surveyor was not even allowed onboard, but he was finally able to confirm that the cargo was aboard and intact, at least as far as could be seen by surface examination. During that visit to the ship, he was made to stand in the hot sun for 4 hours on deck while the Indian Coast Guard "approved his credentials."

The court ordered each insurance company to prove it had paid its claims and had the right to claim against the vessel and the cargo. Documents were obtained from all the companies, including the Dominicans, and presented to the court, but later investigation found the Dominican insurance companies had lied, had not paid their claims, and had no right to the cargo. As a result, we cut them out of the loop entirely and told them they would have to appeal to the court in India on their own. They failed to do so and their cargo was declared abandoned.

Today the *Kobe Queen* is still under arrest, the crew is under guard aboard (and we are feeding them and the guards by court order), the captain's body was taken back to the Ukraine by his wife and the Ukrainian ambassador, the Indian Coast Guard has sued us for $500,000 and was found in contempt of court, the Chennai High Court is accepting bids on our behalf for sale of the vessel and cargo, and three crew members have become ill and are demanding medical care at our expense.

Final bids are due on the 26th—I will be available after this session for anyone wishing to purchase the vessel and inherit this problem. Thank you.

National Security

Stephen Flynn

Commander Stephen Flynn is Associate Professor of International Relations at the Coast Guard Academy. He has been a guest scholar in the foreign policy studies program at the Brookings Institution and an Annenberg Scholar and Resident at the University of Pennsylvania. He is also a Senior Fellow with the National Security Studies program at the Council of Foreign Relations, where he directs a national study group on globalization and the future of border control.

That is a tough act to follow, but it is a nice segue for my presentation on incorporating security into the global system for intermodal freight movements. What we heard from Alan's story are a couple of key elements for those of us looking at this industry and thinking about issues of security, enforcement, and regulation: (*a*) the political boundaries are certainly something we in government have to pay attention to, but they are not something criminals have to pay attention to; and (*b*) the private sector is often the one who gets caught in the middle of all this and often is left with the biggest responsibility to try to handle this. Why? Because we just cannot get there from here in terms of how governments typically operate in today's world. The very changing nature of intermodalism and supply-chain management has made political boundaries basically obsolete, but that is still how we have organized ourselves to try to manage problems of enforcement in crime.

Shortly after the new year, the mass media gave wide coverage of the story of three illegal immigrants who perished their stowaways in a canvas-top container originated from Hong Kong and bound for Seattle. This story was followed by a string of news reports of stowaways discovered in containers arriving in the ports of Los Angeles and Long Beach, all alive but in several instances dehydrated after several weeks at sea.

Just last week, Senator Dianne Feinstein pointed to these incidents, along with a record of seizures of illegal drugs and automated weapons in the port of Oakland, as evidence that "we need much more coordinated federal oversight and additional personnel and technology at America's seaports. Not to do this is really to create a number one target for those who would wish to put our country in harm's way." This was said last week at the Seaport Commission hearings.

Advocates for greater global intermodal development should find the Chinese stowaway incidents and the media and political interests they have generated to be worrisome. The value of modernizing intermodal transportation

networks is tied directly to the expansion of trade and globalization and the corresponding willingness to reduce barriers to cross-border traffic of people and goods. The rise in security breaches is leading to calls for this traffic to be tightly controlled so that the bad can be filtered from the good. In short, not doing enough about security is likened to road support for initiatives designed to facilitate the free flow of trade; however, placing too much emphasis on security could end up undermining the hard-won efficiencies achieved by the intermodal revolution that are so important to the global economy.

How can we extricate ourselves from this conundrum? I suggest a starting point is to acknowledge that exercising tighter physical control over the port of entry is largely meaningless as an end unto itself. Instead, what is central to the public interest is that a capacity exists to advance effective security, law enforcement, immigration control, public safety, and collection of customs duties and fees. First, if we can identify ways to provide these public goods and look beyond our ports of entry as a primary locus of our regulatory enforcement actions, we may have the best of both worlds: improve security and improve the transport of flows of goods and people. This can be done if we are willing to embrace initiatives for managing and policing global intermodal freight networks that place greater emphasis on point-of-origin controls and that provide for near real-time tracking and accountability movements throughout these networks.

A focus on security in the intermodal freight industry is long overdue. Indeed, the private and public sectors who interact with this industry should share the same kind of interest in security that has long been showered on information technologies and the Internet. There is a near-universal recognition that exploiting the information revolution is key to fueling the expansion of the global economy. There is also growing recognition, highlighted by the Y2K problem we recently went through, that many critical elements of our lives depend on the smooth operation of the information age infrastructure. This growing dependence on increasingly sophisticated infrastructures is widely, if somewhat belatedly, seen as a potential vulnerability for the national security posture in the United States.

Cyberterrorism is getting a good deal of attention at the White House, the Pentagon, Langley, and in boardrooms around the country. The result has been the creation of a growing public-private partnership to develop concepts and technologies to protect and defend the information infrastructure against tampering and exploitation. I argue that we need a similar kind of effort for the intermodal industry. However, against a backdrop of robust national conversation about how to derive the full benefits of the information revolution, while tempering risk, the global transportation logistics revolution has been running its course with hardly a whimper. Terms like supply-chain management, warehouse management, and intelligent transportation systems are familiar to this audience, but they are foreign to most politicians, much of the defense establishment, the national intelligence community, the mass media, and the public.

For too long, intermodal issues have been mired in the policy no man's land created by a large and very fragmented industry, as well as the overlapping local, state, regional, national, and international jurisdictions. The National Commission on Intermodal Transportation helped to improve the situation, particularly in raising the profile of the huge economic stakes associated with America's dependence on low-cost and reliable transportation. However, the security stakes link to the intermodal freight industry remains poorly understood. This is worrisome because, as lack of understanding persists, intermodal vulnerabilities may ultimately create a dangerous Achilles' heel.

To date, intermodal modernization has been driven largely by the dictation of the market. To maximize profits, private companies seek out efficiencies that reduce cost. In most instances, where capital costs tend to be very high, the important way to accomplish this is to concentrate operations, reduce overhead, and maximize synergy between components. There are those in the industry who rail against regulatory requirements that presumably interfere with the bottom line and therefore pose a threat to competitiveness. However, when purely market factors determine the development of the infrastructure, important law enforcement and national security interests may be placed at risk.

There is substantial evidence that transportation networks are being exploited by criminals. Conservative estimates place nearly 100 metric tons of cocaine entering the United States last year via commercial air and maritime carriers. Smugglers have gravitated to commercial carriers because they know the odds of successful interdiction are minuscule. In the United States, it takes five U.S. Customs agents an average of 3 hours to inspect a single container. We had over 4 million containers enter the United States in 1996. Maritime container trade is expected to at least double in the next decade. In Hong Kong, more than 500,000 containers are transshipped to all corners of the earth every month. If smugglers can fill just 18 containers with cocaine and smuggle them into the United States, there would be enough cocaine to feed our national habit for an entire year.

Although thugs seemingly benefit from the smooth and efficient operation of large-scale transportation networks, there are others who would reap large political advantage by disrupting it. A growing number of cases suggest that terrorists are finding the transportation sector makes a very attractive target. In summer 1997, New York narrowly averted disaster with the timely arrest of three men involved in a plot to detonate bombs in the

busy Atlantic Avenue subway station in Brooklyn that includes 10 subway lines and the Long Island Railroad terminal. Just 4 years earlier, the police broke up a terrorist cell that planned bombings of the Hudson River tunnels. Overseas, a March 20, 1995, sarin gas attack in the Tokyo subway station killed 12 and hospitalized hundreds.

Instead of targeting the intermodal transportation infrastructure itself, America's adversaries could exploit it to smuggle weapons of mass destruction. Why should a rogue state or a terrorist organization invest in ballistic missile technologies when the weapons of mass destruction could be loaded into a container with a small Global Positioning System device and sent anywhere in the world. Hypothetically, based on current practices in the U.S. Customs Service, Osama Bin Laden could have a front company in Karachi load a biological agent into a container, ultimately destined to New York–New Jersey, with virtually no risk that the container would be intercepted. Under this scenario, he could use a Pakistani exporter with an established record of trade with the United States. The container could be sent via Singapore or Hong Kong, and it could arrive in the United States at the port of Long Beach or the port of Los Angeles and be loaded directly onto bonded rail and truck for the transcontinental trip. Because the entry port is Newark, the U.S. government does not require the cargo manifest to be on file until it actually reaches the East Coast. The carrier has up to 60 days after the goods have arrived to make changes to the manifest, including what and how it was actually shipped. The container could be diverted or the weapons activated anywhere en route long before it was visually identified to be in the country.

My best scenario for Bin Laden if he contracted me would be to ship two boxes to the port of Los Angeles. I would set one off, and then I would say there is another box in the port. Finally, a longshoreman would come in and clean up the mess. We will have shut down trade and also shut down mobilization capacity in most of our Pacific-based operations, which need to run through the same port. We have no plan for dealing with this kind of thing.

In short, for drugs, thugs, and terrorists, the global transportation logistics network provides an unparalleled means to move about and wreak havoc with virtual impunity. The public will not tolerate the situation. I suggest over the long run that serious thought be given to incorporating security into the modernization of the intermodal freight industry. Accordingly, attention will be required at three levels:

- First, we need a security regime that provides strategic depth. Specifically, governments and the private sector must work together to create the capacity for a point-of-origin system of safeguards and inspections by placing primary reliance on the port of entry approach. The premise of this recommendation is that, once the river of commerce arrives at our borders, it cannot be effectively policed. Targeted measures that reduce the risk of smuggling and terrorist activities when goods first enter the streams of trade is a more practical approach to take.
- Second, trade needs to be increasingly more transparent. Manufacturers, freight forwarders, carriers, importers, and retailers who use the global transportation logistics networks must be willing to closely track the movement of goods and people throughout these networks and make relevant information readily available in useful formats to regulatory enforcement authorities. This will enhance the ability of those with authority to conduct virtual audits of these movements and to act quickly when they have intelligence about potential compromises. This is not a call for creating new layers of red tape but a suggestion that border control agents move away from 19th century paper-based regulatory enforcement processes and toward 21st century information-age tools. Most of these tools are in place, particularly in the private sector, where firms have invested in the kinds of communication, data management, tracking, and navigational technologies that can help improve the overall efficiencies of their operations. Too often there is a tendency on the part of border control agents, in the United States and abroad, to not think about how best to apply technologies that can achieve the ends of trying to ensure the public safety and security and collect duties and so forth, with the logic of the system itself and how it operates.
- Third, appropriate incentives and sanctions must be marshaled to promote and sustain a new regime within the private and public sectors. Incentives for the private sector should include conditional facilitation for those participants in the global transportation logistics networks who embrace the first two elements—that is, tightened port origin security and in-transit transparency. Once this capacity is verified, these shippers and carriers should be allowed to move through the equivalent of a trade and travel "E-Z lane," where they garner the benefits of low transportation costs and faster movements by reducing the risk of delay, spoilage, and wreckage at border entry points. Regulators and enforcement officials would continue to conduct spot checks to ensure compliance, but the overwhelming majority of these goods and people will be allowed to travel with few restrictions. Private sector actors who are unwilling or unable to ensure point-of-origin and in-transit security and transparency would be subjected to the slow lane of traditional inspections and administrative hassles as they move across borders. Similarly, private sector actors who have signed up to the regime but are found to have failed to comply with its mandates would, at a minimum, face the sanction of being placed back in the slow lane.

The essential argument being advanced is, going back to the Internet analogy, that there has been about a 10-year battle by the National Security Agency and the FBI to put a clipper chip, an encryption key, into web communications. What they recognized, somewhat belatedly as the use has proliferated, was that one of the basic forms of surveillance, wiretaps, could no longer apply if people were on the net. What they tried to do, after the fact, was go in and put this security system on as the system was being modernized. Finally, just this past fall, the Administration threw its hands up in the air because, as probably most of you know, the encryption technology we are trying to prevent from being distributed actually was put on the web, PGP encryption technology, for anybody who wanted to sign up and download the thing. It took 5 years after that event for the government to acknowledge that we could not do this; hence, they have simply given up.

A core problem with organized crime is that you have to prove the conspiracy of a crime. The very nature of organized crime is that the hand is not in the cookie jar. What you have to show is that people have come together in the conspiracy and the only way you can do that is with an informant or by surveillance. However, as technology has changed, we have no ability to do surveillance anymore. Basically in today's environment, we find ourselves saying, "Well, I guess we will live with organized crime and the inability to do surveillance," while the kind of operations that Alan just described continue to proliferate.

In the intermodal industry, there is an opportunity to start thinking about putting security into these systems and making sure they cannot be infiltrated by bad guys, both in terms of cargo theft and putting into cargo shipments things that could do tremendous damage, such as weapons of mass destruction. The private and public sectors will have to work in cooperation; however, it appears that at present the private sector does not want any interference, does not want any government involvement in security, because it will slow down the flows and disrupt the bottom line. The repercussions of that may be that, at the end of the day, the logic of the marketplace may prevail and government can no longer provide security for that system. Then we are going to be back in the Middle Ages, where the private sector will have to hire its own security to essentially ride posse with its goods as it moves through the global transportation network because the public sector can no longer do it for them. That clearly is not a desirable end state.

In the interim, we are also faced with the reality of increasing backlash to globalization, as observed recently in the response to meetings of the World Trade Organization. If the public starts to believe that public goods are not being managed as we speed up our global economic interaction, they may be much less supportive of facilitation. That would be a problem for this industry and we are already seeing signs of that. If the neoprotectionists can point to security breaches, such as terrorists coming into a port or drugs and weapons flowing in and out of ports, you are not likely to get a whole lot of support for further facilitation initiatives.

The bottom line is that the private sector has a vested interest to work with the public sector to get this right, and the public sector clearly has a vested interest to get this right, because we cannot do it within our own narrow jurisdiction. Most of the action is taking place in the private sector and will require excellent cooperation. Thank you.

Crime and Security in U.S. Seaports

John McGowan

John McGowan is Executive Director for Field Operations in the U.S. Customs Service, and is currently detailed to the Interagency Commission on Crime and Security in the U.S. Seaports. He has held numerous positions during his 30-year career with Customs, where he was directly responsible for the control of crime and security to air, rail, and sea terminals around our country. He has a very intermodal perspective from the federal government side.

I am here to talk about the activities of the Interagency Commission on Crime and Security at U.S. Seaports. However, I would first like to comment on the previous presentations from the perspective of U.S. Customs. Alan Spear spoke about an event that basically involved people who were not who they said they were, who were masquerading as someone else, with intentions that were not as originally stated. Commander Flynn spoke at a higher level of the system that moves goods around the globe and how it functions logistically versus how it functions through other methods—guarantees for transparency, safety of movement, security of movement, and what needs to be addressed to enhance that.

Customs is not interested in holding on to our red tape. Fifteen years ago, we went forward and paved our "cow paths" by automating a number of systems. We continued to do the work we had been doing for 200 years the same way, but we did it in an electronic medium instead of on paper. We are more than willing to take the next step and change what we do and how we do it. We have enabling legislation that took 5.5 years to get through the congress. We are ready to use it to its full extent. We are stymied and we have a scheme that is unfunded. Why? Because not enough people understand

the next steps, not enough people understand that to make this breakthrough statement about how the control agencies are going to control goods entering or departing a sovereign nation, it is still going to be a function that occurs at borders, at ports of entry and ports of exit. Not enough people understand much of what we do, how intrusive it is, how onerous it is, or how it can be changed and how it can be enhanced, and that to do so is going to take money and it is going to take strategic thinking to get the monies into the flow soon.

To borrow an Immigration and Naturalization Service term for a moment—malifides. Does everybody know what that is? I do not even know if that is a real word or a real translation from Latin, but it is what the Immigration and Naturalization Service uses to talk about people whose intent is different than what they say. Someone personally shows up at the border and has a tourist visa, but his intention is to overstay. His intention is to illegally enter the United States. He is a malifide—he is not stating his true intent. That is what we deal with on a regular basis that costs us inordinate time and effort. The good news is that only a very small percentage of the people you encounter are malifides; the bad news is the inordinate cost in time and resources that are spent when you run across somebody who is a malifide.

Now let me get on to my presentation on the Interagency Commission on Crime and Security at U.S. Seaports, which was established in April 1999. It was an outgrowth of the discussions and activities surrounding the marine transportation system referred to by previous speakers. The commission is cochaired by the Departments of Justice (Office of the Attorney General), Treasury (U.S. Customs), and Transportation (Maritime Administration). Other federal agencies, some of whom were control agencies and some of whom had issues with control agencies, are also involved. The Department of Defense and Joint Chiefs of Staff are represented because of the strategic involvement on outload ports. The Office of Management and Budget; the Departments of Agriculture, Commerce, Labor, and Health and Human Services; and the U.S. Environmental Protection Agency also have an interest in what are the control functions and security aspect of the ports. Although this is a federal commission, we also gather inputs from state and local governments and from the private sector.

The objective of the commission is stated in the memorandum of the commissioners who are establishing the commission. It will look at the nature and extent of crime in seaports, the overall state of security at seaports, and the mission and authority of the various agencies—how they are interlinked, who has what authorities, what is their mission, why do they have those authorities, and how do they carry it out. It is also looking at the effectiveness of coordination between the federal agencies and the state and local authorities. Do they communicate? We needed input from stakeholders and recommendations to enhance the state of security in seaports.

In the past year, a dozen on-site visits have been made to major U.S. ports. Staff have also conducted focus groups with over 45 groups and conducted interviews with more than 300 people. Input was also gathered from more than 1,000 other people who had business at our offices or by phone or letter. The commission also established a website, put notices in the *Federal Register*, and met with everybody who uses a port or who makes their money in a port, including freight forwarders, terminal operators, and vessel and carrier operators. Observations were made at the 12 ports and there was also some benchmarking on what is going on in Europe—specifically in the United Kingdom and the Netherlands—to see how other people run their ports and how they function. They have the same control functions and security functions but different underlying legislation.

We found that most of the crimes at seaports are federal crimes, with no reporting mechanism. State and local jurisdictions do not report seaport crime, and they do not report transport crime. They report crimes against things and persons. If it is a robbery, it is a robbery. If it is a theft, it is a theft, but they do not distinguish it from any other thing that happens in their jurisdiction. Therefore, it is very difficult to try to get a handle on state and local crime that might occur in seaports. For the most part, those state and local authorities say this is a federal crime so it is your problem, not ours. Statistics reveal that a lot of things that go on in seaports fall under the various federal statutes and the federal environment.

One of the first recommendations from the commission will focus on standardization, some sort of mechanism for better reporting and better collection of information so that the actual threat and the actual vulnerability can be better assessed.

Internal conspiracies involving contraband such as cocaine and marijuana were found to be a huge problem in southern Florida, particularly the port of Miami, but it is spreading to other ports. Basically, people who do not have the right to do so are accessing the cargo to remove their contraband—someone at the other end had similarly accessed cargo to place the contraband. You have a legitimate shipment going from a legitimate manufacturer to a legitimate consignee and somebody is getting a free ride along the way for their contraband. Something is put in at one interim point and taken out at another interim point in the cargo movement—an internal conspiracy.

There is a need for more intelligence and information sharing among agencies. Increasingly we hear about the need for better communication, coordination, and cooperation, but in the case of seaport crime, we found this was to the extreme—nobody was talking about what each of them was doing within the same environment.

There need to be more vulnerability assessments at ports. Ports often do not understand the threats facing them, because they have not been told by the various federal agencies why or how the seaport environment was vulnerable. They have not been briefed by Customs on what Customs was encountering in the port as a locust. They have not been briefed by the U.S. Department of Agriculture on what the threat of pests was in its entirety, or on a scale from 1 to 15 in the ports throughout the United States.

There are no accepted standards for physical security—how high should the fence be, how many illumines should you have in the lighting environment, how many gates are appropriate for what throughput. Nothing like that exists right now. If somebody were to ask what is the assessment of security at seaports, it goes from fair to poor or from fair to none. There are individual exceptions. You have very secure private terminals; for example, the oil terminals are exemplary and could perhaps be held out as a benchmark for others to look at—the way they identify who gets on their terminals and who stays on their terminals and what they do while they are on their terminals. However, it is not security driven—nobody goes off with 63,000 barrels of oil in their back pocket—it is safety driven. Nonetheless, it is the same control aspect.

Access to seaports is relatively uncontrolled. I recall working in Newark, where there was a public boat launch ramp. You could drive through an active port—anyone could drive out and launch their ship, their vessel, or their little runabout into the Newark Bay.

Coordination and cooperation among agencies are fragmented, which inhibits the sharing of information mentioned earlier. There is a need for coordinated action and activity among the agencies.

Security-related meetings are not held in most ports. There are lots of business meetings and meetings with ad hoc groups to discuss problems such as paving, gates, and other operational aspects, but rarely, if ever, do people come together on a regular and routine basis to focus on port security agenda.

Equipment and technology are lacking at many ports. The technology is out there for nonintrusive inspections and U.S. Customs is becoming interested in being able to scan full containers. You may recall that Commander Flynn mentioned it takes five inspectors 3 hours to discharge a container looking for contraband. If Customs had a scanning device that could do that in 15 minutes, it would be an enhancement to productivity and to security. The technology exists, but it is either not funded, it is underfunded, or it has not been deployed in the right place within specific ports.

There were some common themes that came out of the port visits and the focus groups. The crimes they most often concerned themselves with were vandalism, theft of their equipment, destruction of their facilities, pilferage, stolen automobiles, and things like that. We heard a lot about cargo theft and cargo crime, but for the most part, with the advent of global intermodalism, it often does not occur on the port anymore; however, the information about what container to steal generally does come from the port. Somebody on the inside is telling somebody on the outside—the frequency with which the high-value load gets ripped off versus the container of dishwashing detergent is not a result of blind luck. A lot of coordination is needed to know what is in a container, where it is parked, when it is unattended, and when it is moved, before it disappears.

A lot of the equipment that contains high-value cargo is found in or near the port environment, which suggests that a lot of it is destined to foreign locations—a load is lost after leaving the port of Los Angeles, but an empty truck is found in New York. What was going on? The Interstate highway system was the conduit that enabled the movement, but the seaport was the ultimate outlet to a foreign market. Thieves most likely changed the nature and the condition of the cargo to a point where it was not identifiable as stolen cargo and it went for a good sale.

There are a lot of recommendations with respect to controlling port access by identifying people through identification cards. This is a big topic with organized labor in U.S. ports. They do not want criminal history checks performed on them, but when I listened to people representing the insurance industry, they said that everybody should do preemployment screening. Everybody should have the ability to do some sort of background checks. What the commission is going to have to come to grips with is the depth of the recommendations. Many people believe there should be deep criminal history checks done on everybody who works in a port, everybody who works in the receiving clerk's office, everybody who works in the shipping clerk's office, and everybody who works for the insurer—all these people should be investigated to the *n*th degree. However, when you look at that cost and expense, maybe it is the right people have to have such background checks done only when there is cause. Identification procedures and control of access to areas where critical information is gathered and stored, to cargo makeup areas, and to cargo breakdown areas do make sense.

The need for cooperation includes getting more information from the federal agencies, who should take the lead in gathering information, but not through regulatory action or legislative action. The stakeholders are looking to federal agencies for guidelines, through consistency, through a commitment of time and resources in talking about what they know that we do not know and vice versa. When talking about cargo crimes, there is little interest in sharing information about what is happening in a particular port because that might put the port at a dis-

advantage if it gets the reputation of being a criminal-laden port. Although such information should not be broadcast, it should nonetheless be gathered and analyzed, so that aggregate trends can be shared among users—this may be an appropriate role for the federal government.

The commission staff is evaluating the observations, identifying significant issues, and preparing recommendations through the three cochairs from the departments. These will be presented to the Attorney General, the Secretary of Transportation, and the Secretary of Treasury, who in turn will convey them to the White House for action. There is considerable congressional interest in the findings and recommendations of the commission, which is focused on coming to grips with reasonable, viable, affordable recommendations behind the observations.

One final comment relating to a recurring theme heard at this conference—specifically, port throughput, the speed of cargo transfers, and so forth. From my perspective in Customs and from the perspective of a lot of the federal agencies who look to the ports to be a controlled point, give our issues the same weight you give your issues when you are thinking about what you are building. I looked at the mission of the Transportation Research Board and what they are supposed to be doing. If we go back and review some of the comments made by Commander Flynn, I suggest that the future work, the future action agenda, should be how to achieve the desired throughput in ports, while keeping the necessary border and port of entry controls that an autonomous nation requires for both inbound and outbound movements. Thank you very much.

Cargo Theft and Liability

Jeff Black

Jeff Black represents the Technology Asset Protection Association (TAPA). He is currently employed with Micronpc.com after 18 years as a criminal investigator for the Idaho Department of Law Enforcement. He joined Micron to establish a fraud unit within the security department and has moved up through various management positions to his current position as operations and support manager with the responsibility for physical and logistical security, investigations, planned operations, document systems, risk management construction, and leases and contracts. He is also a former Coast Guardsman.

I am here today to discuss the formation and guidelines of TAPA, the Technology Asset Protection Association, which is composed of the security directors of the top 60 high-tech companies in the United States. The organization was founded because we were all "mad as hell and not going to take it anymore." We came together in summer 1997 as security directors and said, "Because of cargo theft, we are unable to get the raw materials to manufacture our products for shipment to our customers. As a group, what are we going to do about it?"

All of us had gone to various law enforcement entities and various other organizations seeking help. As a group, we realized that approach was not working and that we would have to step forward, take things into our own hands, and do something about the problem—the result was TAPA.

The combined revenues of the companies within TAPA total about $760 billion. TAPA is a nonprofit organization, initially organized by representatives from Intel, Compaq, and Sun Microsystems. We now have 135 members representing 60 high-tech companies. Currently, we are generating a lot of interest throughout the United States and around the world. We have had three feature articles in the *Journal of Commerce*. We were a featured article in the *Investors Business Daily*, and we have been speaking and publishing in various logistics and security trade venues and publications.

We have ongoing liaisons with different freight forwarder and carrier groups, including Cargo 2000, Air Transportation Association, National Cargo Security Council, American Trucking Associations, and insurance underwriters, the latter a relationship we are developing throughout the world. We recently had a law enforcement summit in January 2000 in Washington, D.C., that brought together the FBI, U.S. Customs, and U.S. Treasury Department and asked them to work with us to determine how to work out these issues.

Among our objectives are the development and utilization of common tools for freight security, regulations, contract language, and auto-protocol. We are separating our rates from our security guidelines. Historically, when we were talking with our transportation carriers, it was always about rates. What are you going to do for us? Contractually, we were obligated when there was a loss to a certain recovery. What we are doing now is separating the rate conversation from what are you doing security-wise. We are increasing security awareness and communicating best practices.

One of the things we are doing is benchmarking within our own group. We have all signed nondisclosure agreements with one another and are using a company called Asset Management Group. Within TAPA, we have our own benchmarking group, which measures where we are from our losses on a quarterly basis. We also identify our best practices and distribute that information to our membership. We communicate information on the volume and the attractiveness of high-value cargo to criminal elements, particularly violent criminals. We develop performance

measures of existing supplier bases and create a market niche for interpreters.

We are telling companies out there that if they are adopting best-known security practices, we will work with them and we will move our supply chain toward their companies. If they are not willing to work with us as an organization or as individual companies concerning their freight security guidelines, there are other companies out there that will do that. We are trying to establish some standard forms to evaluate effectiveness. We are constantly pursuing further improvement and setting future agendas about where we want to go as an organization.

In forming freight security regulations for 1999, TAPA basically massaged the model developed by Intel and adapted it to fit the various organizations that represent TAPA. One important issue we are discussing is product packaging. One of the things that drives security directors nuts within the industry is that we more often than not list everything that is inside the box on the label. Thieves at various parts of the supply chain can look at that box and if that is what they want, they take it. I am sure everybody in this room can spot a Gateway box—a great big black-and-white cow box. You go into a United Parcel Service terminal or you go into a freight forwarder and you can see that Gateway box all the way across the room. The same thing with the packaging used by Dell and Compaq. The companies are telling the bad guys what is inside—security directors are looking internally at what we can do as organizations to minimize that.

This year we are working toward developing an independent auditor pilot program with volunteer freight forwarders and carriers that would minimize multiple audits on the freight forwarders and the carriers throughout the United States. Right now, Intel goes out and audits a freight forwarder, then I come in and audit that same freight forwarder. All my competitors go in and audit that freight forwarder. From a security standpoint, our organization proposes to hire independent contractors. TAPA will establish the guidelines and has already established the protocol. The contractors will go in and perform the audit and then report back to TAPA on the findings from a particular audit. This will minimize the impact on that particular carrier as well as the time that each individual member would have to spend to go out and do this.

TAPA is considering classifying facilities in three basic categories, depending on the level of threats. The threat level of a transportation company in Boise, Idaho, is totally different than one in Miami or in Los Angeles, Seattle, or Chicago. We are looking at the environmental as well as the historical data concerning the area where a freight forwarder or a logistics company is located. We are looking at trucking operations on a 1 to 4 scale. What are they hauling? How big a company is it? Where are they located within the United States? We are doing an assessment protocol using a quantitative score with no weighting. We are also looking at what we call the V-3 philosophy—value, volume, and vulnerability—when we assess a company. We realize that, within the business, we must look at each of the groups being audited in a different light. We know we can set a national standard and expect every carrier out there to meet that because, depending on what they are hauling, depending on the volume they are hauling, and depending on exactly where they are located in the United States, it is going to have an impact.

When we started Micronpc.com several years ago, we were dealing with just-in-time inventory where we would have sometimes 15 to 20 days of inventory on site. Now, we all know that inventory is the work of the devil, so we are constantly trying to reduce the amount of inventory we get on-site and we went to barely just-in-time inventory. We have supplier hubs across the street and we qualify the product over there and we bring it in on time. Now we are moving into just barely just-in-time inventory where our goal, in a sense, is to get our inventory down to having on premises no more than 3 to 6 hours of inventory in a manufacturing cycle. Our competitors, of course, are doing exactly the same thing, so the disruption within the supply chain is absolutely huge. It is not just that when we are working with a vendor hub and therefore do not own the product until it gets to our facility. Quantum owns the hard drives until they get to the supplier hub and before they get over to us. The issue is not that if we lose a truckload of Quantum hard drives between the Bay area and Boise, Idaho, we are going to file a claim with our insurance carrier. The issue is that we do not have a truckload of Quantum hard drives to put in the PCs being sold to customers. From one aspect it is an insurance issue, but insurance does no good if we do not have the parts in our hands to put in the PC to put on a truck to sell to the customer.

The customer impact on just-in-time processing is huge. In a direct-market model, everything we manufacture is sold before it goes out the door. We must have that customer commitment that when we tell them a PC is going to be on their doorstep or it is going to be in their business at a particular time, it is going to be there. As soon as our supply chain gets interrupted, it has a tremendous impact that both we and our customers can appreciate.

With respect to vulnerability, one of the things we are doing as an organization is looking at what is valuable and what is hot in the black market, and how, in a sense, that has an impact on us. As the price of D-RAM dropped all the way down to about $5.00 a megabyte, hard drive prices went up. They became the absolutely hottest item out there. That is but one example of how we look to see what is the hottest product out there on the market and how are we going to protect it.

For those who are interested, I can provide a copy of the freight security guidelines electronically. It will give you an idea of what we are looking at and how we are rating, in a sense, companies throughout the United States. We talk about the freight security requirements, the contractual language, the standard assessment protocol. We talk about the consequences, the corrective actions that need to be taken. We talk about training the employees within the companies with whom we are dealing. We talk about the investigations and the investor's role in responsibilities for the losses.

We believe that freight security models, contractual language, standard assessment protocol, and freight security requirements must be incorporated as elements in our contracts in order for this to be successful. The high-tech industry will not be able to sustain the losses that we have in the past and we are not going to do it. We are taking on a new role with respect to audits. We are going to start rating companies. We are going to determine who is providing the security out there so that we can get our product to market and we can get our raw goods into the manufacturing sites.

We are moving forward on this. When we started this organization, no one believed we could do it. After 2 years, people are starting to listen and they are starting to realize that we, as an industry, with respect to that $740 or $760 billion worth of revenue in this country believe we can have an impact on how freight is handled within the United States and outside the United States, as reflected by the fact we are also expanding into Asia, Latin America, and Europe. Thank you very much.