AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 107–309

WEAK LINKS: ASSESSING THE VULNERABILITY OF U.S. PORTS AND WHETHER THE GOVERNMENT IS ADEQUATELY STRUCTURED TO SAFEGUARD THEM

HEARING

BEFORE THE

COMMITTEE ON
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

DECEMBER 6, 2001

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

78–045 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia
THOMAS R. CARPER, Delaware
JEAN CARNAHAN, Missouri
MARK DAYTON, Minnesota

FRED THOMPSON, Tennessee
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
ROBERT F. BENNETT, Utah
JIM BUNNING, Kentucky

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
DAN FELDMAN, *Counsel/Communications Adviser*
JASON M. YANUSSI, *Professional Staff Member*
HANNAH S. SISTARE, *Minority Staff Director and Counsel*
JAYSON P. ROEHL, *Minority Professional Staff Member*
DARLA D. CASSELL, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Lieberman	1
Senator Levin	3
Senator Collins	15
Senator Cleland	30
Senator Bennett	33
Senator Thompson	36

WITNESSES

THURSDAY, DECEMBER 6, 2001

Hon. Ernest F. Hollings, a U.S. Senator from the State of South Carolina	6
Stephen E. Flynn, Ph.D., Senior Fellow, Council on Foreign Relations and Commander, U.S. Coast Guard	10
F. Amanda DeBusk, Miller and Chevalier, former Assistant Secretary of the Commerce Department and former Commissioner, Interagency Commission on Crime and Security in U.S. Seaports	16
Rob Quartel, Chairman and Chief Executive Officer, FreightDesk Technologies and former Member, U.S. Federal Maritime Commission	19
Rear Admiral Richard M. Larrabee, Ret., Director, Port Commerce Department, The Port Authority of New York and New Jersey	23
Deputy Chief Charles C. Cook, Memphis Police Department	40
Argent Acosta, Senior Customs Inspector, Port of New Orleans and President, National Treasury Employees Union (NTEU) Chapter 168	43
Michael D. Laden, President, Target Customs Brokers, Inc.	47
W. Gordon Fink, President, Emerging Technology Markets	49

ALPHABETICAL LIST OF WITNESSES

Acosta, Argent:	
Testimony	43
Prepared statement	127
Cook, Deputy Chief Charles C.:	
Testimony	40
Prepared statement	120
DeBusk, F. Amanda:	
Testimony	16
Prepared statement	93
Fink, W. Gordon:	
Testimony	49
Prepared statement	138
Flynn, Stephen E., Ph.D.:	
Testimony	10
Prepared statement with an attachment and slide presentation	57
Hollings, Hon. Ernest F.:	
Testimony	6
Laden, Michael D.:	
Testimony	47
Prepared statement	133
Larrabee, Rear Admiral Richard M., Ret.:	
Testimony	23
Prepared statement	114

Page

Quartel, Rob:
Testimony 19
Prepared statement with slide presentation 98

APPENDIX

Slide presentation by Stephen E. Flynn entitled "Bolstering the Maritime Weak Link" 80
Slide presentation by Rob Quartel 107
Letter (with an attachment) to Senator Collins from Captain Jeffrey W. Monroe, Director, City of Portland, Department of Transportation, dated October 26, 2001 142
U.S. Customs Service Optimal Staff Levels, Fiscal Years 2000–02, February 25, 2000 148
Classification of U.S. Customs Districts and Ports for U.S. Foreign Trade Statistics 285
Responses to questions for the record from:
Mr. Flynn 248
Ms. DeBusk 253
Mr. Quartel 259
Rear Admiral Larrabee, Ret. 270
Mr. Acosta 275
Mr. Laden 277
Mr. Fink 282

WEAK LINKS: ASSESSING THE VULNERABILITY OF U.S. PORTS AND WHETHER THE GOVERNMENT IS ADEQUATELY STRUCTURED TO SAFEGUARD THEM

THURSDAY, DECEMBER 6, 2001

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:08 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Levin, Bennett, Cleland, Torricelli, Collins, and Thompson.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning. Thanks to all of you for being here, particularly to Senator Hollings and our other witnesses. This is one of a continuing series of hearings that this Governmental Affairs Committee has held since the terrorist attacks of September 11 which have examined the Federal Government's ability to prevent, prepare for, and respond in the event of future terrorist attacks.

In some ways, we ask questions that some have been hesitant to ask in the past, and I suppose some might wonder why we are asking them now—because they may reveal vulnerabilities. And yet, if we do not ask them, we will not close those vulnerabilities and we will be susceptible to further attack. I think all of us felt that, unfortunately, after September 11, we have to start thinking more like the terrorists do, and we are going to try to do it in a very thoughtful and comprehensive way today and we have the witnesses here to make that happen.

Not since December 7, 1941, which is 60 years ago tomorrow, has the question of our domestic security so dominated national debate. The Committee has taken a hard look at whether the Federal Government is appropriately structured to meet those challenges. Specifically, we have held hearings on our aviation and postal systems, on cyberspace, and more broadly, on the safety of our critical infrastructure and how we should organize for homeland security.

Today, we direct our attention to the security of the Nation's 400-plus ports through which 95 percent of all U.S. trade flows. The picture, unfortunately, is not a reassuring one. U.S. ports are our Nation's key transportation link for global trade and yet there are no Federal standards for port security and no single Federal agen-

cy overseeing the 11.6 million shipping containers, the 11.5 million trucks, 2.2 million rail cars, 211,000 vessels, and 489 million people that passed through U.S. border inspections last year.

I just want to put an exclamation point there, that as I have studied this more, I must say it surprised me. There are no Federal standards for port security and no single Federal agency overseeing port security. Port security is largely a matter of State and local administration. The Coast Guard, the Customs Service, the Immigration and Naturalization Service, and other agencies all have a role to play, but the plain fact is that the movement of goods into the United States, five million tons a day, is now so efficient in the sense of goods coming into the country and moving rapidly as a matter of commerce to their destination that port security has been sacrificed.

It is not possible to physically inspect more than a small sample of containers as they arrive in the United States. Less than 1 percent are actually examined, and that leaves our ports, unfortunately, vulnerable to attack. And not just our ports. Containers arriving from Europe, Asia, or Canada are more likely to be inspected at their final destination rather than at the arrival port.

I am sure that would surprise most Americans, but that is the reality and it means that at any given time, authorities have virtually no idea about the contents of thousands of multi-ton containers traveling on trucks, trains, or barges on roads, rails, and waterways throughout the country. The ease with which a terrorist might smuggle chemical, biological, or even at some point nuclear weapons into one of those containers without being detected is terrifying.

Even the physical security of ports is minimal. Last year, the Commission on Crime and Security in U.S. Seaports reported that of 12 of the Nation's largest ports, 6 had perimeter fencing that could be penetrated, 4 had no regular security patrols, and 10 never performed routine criminal background checks on employees. The Commission said the state of security, "at U.S. seaports generally ranges from poor to fair."

The FBI told the Commission that ports were highly vulnerable to terrorist attack, although at that time, they considered the threat to be marginal. The assessment, of course, has changed since September 11 and 2,000 military reservists have now been activated to shore up port security.

Part of the overall problem, as is so frequently the case, is the lack of resources to properly enforce port security. But, of course, we are going to be dealing with that on the Senate Floor in the Department of Defense appropriations bill and the homeland security funding that is part of that bill.

The Coast Guard, for example, has 95,000 miles of shoreline to patrol but is at its lowest level of manpower since 1964. International trade has doubled since the mid-1990's, but the number of Customs inspectors has remained the same, just 8,000. The Federal Government is also handicapped by a lack of coordination and communication between agencies.

I have heard that a ship with a—this is a hypothetical, but not too improbable—a shadowy record of ports of call, for example, carrying a cargo that does not square with its home port and manned

by crew members on a watch list of people with suspected terrorist ties might not necessarily raise any red flags, and that is because the Coast Guard could know about the ship, Customs could know about the cargo, and INS could know about the crew members, but no one would necessarily have all that information, so the pieces would not be pulled together to form a picture that would set off alarms.

Even if resources and coordination were adequate, the front-line agencies would still be handicapped by a lack of access to national security intelligence from the FBI and the CIA. That is a complaint that I have heard over and over again from local officials following the September 11 attack.

The Committee is particularly pleased to welcome Senator Fritz Hollings and to thank him for his leadership and dedication—lonely, most of the time—to pursuit of better port security in America and the critical role that he has played in keeping this problem on our collective radar screens over the years. I am very pleased that he is with us today to testify about legislation that he and Senator Bob Graham have written to respond to the vulnerability of our ports. Their legislation, which I strongly endorse, addresses some key findings and recommendations of the Commission on Seaport Security. Our ports, goods, and citizens will be safer when it passes.

I must say that the more that I study this issue, the more I realize how pervasive the problem is and how much work we have to do on it to make sure that we get our entire system of importing and exporting to a point where it is not only efficient, but it is also safe. The entire commercial structure may need to be addressed systematically, and as some of the witnesses we are going to hear this morning will suggest, the best answer may lie in an entirely new approach that relies on innovative technologies combined with security inspections starting at ports of origin, rather than ports of destination. I am going to be very interested to hear testimony on that.

We may need, as one of our witnesses would put it, to push our borders back and create sanitized shipping zones for goods bound for the U.S. from overseas ports. We certainly need to put technologies to work so that containers can be electronically sealed and alarmed after they are inspected, then X-rayed for a baseline record of their contents. Global positioning satellite systems could be attached to all containers to monitor shipments, and a secure Internet tracking system could help place a shipment anywhere along its path.

Fortunately, our ports are busy and they do not need a bail out. They just need a sensible strategy to keep them safe and sound as vital economic hubs, and I am hopeful that the testimony we will hear today will help the Congress do just that.

Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Mr. Chairman, thank you. Thank you for these series of hearings that you are holding that are really a comprehensive series, and I think perhaps the most comprehensive

look that is being given to our security issues in a whole host of areas.

I also want to join you in welcoming Senator Hollings, an old friend of both of ours, or a dear friend, I should say, of both of ours. He has been, indeed, a leader in the subject that you are looking at today.

We, who are on the Northern Border, are particularly very keenly interested in this subject. We have twice the Border as exists on the South Borderand yet we have a small, tiny fraction of the security which exists there, and that is inadequate, and you will be hearing more about that. The Northern Border receives about two-thirds of the truck traffic, about 85 percent of the trains, a large number of ships.

We have the longest coast, actually, of all the four coasts. People sometimes forget that the St. Lawrence Seaway and the Great Lakes is the longest coastline that we have in this country. We have many ports of entry, lots of ships coming in from overseas, and it is a major issue for us. The issues that the Chairman has identified, are both the security issue as well as trying to move trade, because when we have long lines of trucks, for instance, coming into my home State and leaving my home State, with trade, it means that our plants are not able to run as efficiently when we have to wait 2 or 3 hours at a bridge or a tunnel. What you are looking at today is mainly seaports, but I gather you are including all ports of entry, and I think the third panel will be looking at those, as well.

What you have identified, Mr. Chairman, one of the issues that we are pushing very hard on is the reverse inspection issue. It makes a lot more sense to be inspecting cargo before it lands at our ports, before it goes through our tunnels, before it goes across our bridges, because it could be too late. If someone wanted to attack a port or a tunnel or a bridge, they would do so before they entered our country, not afterwards, and they would do it in the process of entering, not after they have entered.

So the reverse inspections that we are pushing so hard for, getting our Customs people to get involved in much more actively, could be an important part of added security for our ports of entry, including our bridges and tunnels. Some of the technologies which the Chairman has identified are also very important and we must put more resources into those technologies to identify threats to our ports of entry.

And also, we need more resources. We have a huge shortage of resources, particularly on the Northern Border, but I think that is true on the South Border, and also on the East and West Coasts. We have a large number now of temporary employees following September 11. We have got to have permanent employees instead of temporary employees. But we have both resource problems, technology challenges, and just plain common sense that push for those reverse inspections that could provide so much greater security.

But while I must leave you, Mr. Chairman, I am very keenly interested in this subject. I want to again thank you for these hearings. I congratulate Senator Hollings for his usual steadfastness in staying with an issue for so long, and I think that, finally, tragically, probably, because it took September 11 to wake us up, but

nonetheless, finally, I think we are going to get to the point where Senator Hollings has been for so long.

PREPARED STATEMENT OF SENATOR LEVIN

It took the tragedy of September 11 and the subsequent need for heightened security along our borders to draw attention to what many of us have known for years; there is an alarming lack of resources along our Northern Border. While much has been done over the last decade to improve security on our border with Mexico, the Northern Border has largely been ignored. For example, only 1,773 Customs Service personnel are present at our border with Canada, while 8,300 protect our Southern Border. Similarly, while 8,000 Border Patrol agents monitor our 2,000 mile Southern Border, only 300 are stationed at our 4,000 mile Northern Border. So, 96 percent of our Border Patrol agents are assigned to a border that is only half as long as the one to which 4 percent of agents are assigned.

Although hugely understaffed, we process a large percentage of the country's commercial traffic. The Northern Border has six of the top eight truck border crossings in the country, including the number one truck border crossing, Detroit's Ambassador Bridge. Our Customs officers on the Northern Border process 62 percent of all trucks, 85 percent of all trains, and 23 percent of all passengers and pedestrians entering the country each year. However, our Customs inspectors represent only a small fraction of the currently deployed inspectors in the country, and their numbers have remained essentially static since the 1980's.

The Detroit Region has half of all Northern Border crossing traffic yet has only 10 percent of the INS inspectors assigned to the Northern Border and 24 percent of the Customs inspectors assigned to the Northern Border.

With this startling lack of resources, it's no surprise that the new security measures at the border have a tremendous impact on our region's economic well being. Auto plants wait days for critical parts. Hospitals can't perform vital services when supplies and staff are trapped in long lines at the bridge and tunnel. We need to find a permanent solution to the staffing shortfall at our borders so that we are able to perform essential security inspections without causing unreasonable backups that hurt our economy. We are grateful for the recent Federal commitment to increase the number of National Guard at the Northern Border and are relying on them to help protect our border and keep traffic and commerce flowing smoothly. However, we need to move quickly to put permanent staff and technology in place.

Congress has taken some important steps to achieve this goal, but we are not there yet. The FY 2002 Treasury Postal Appropriations bill provides an additional $28 million for Customs to institute a Northern Border initiative including hiring approximately 285 additional Customs officers. The Commerce Justice State FY 2002 Appropriations bill provides for $66.3 million for 570 new border patrol agents across the nation and $25.4 million for 348 new land border ports-of-entry INS inspectors across the nation. Particular attention will be paid to the needs of the Northern Border. Congress also tripled staffing levels for INS, Customs and Border Patrol staffing on the Northern Border in the anti-terrorism bill. A portion of the $40 billion emergency supplemental should also go to staffing up the security at our Northern Border.

But improved border security involves more than just more money. It requires changing policies and practices that don't make sense. On November 13 I held a hearing of the Permanent Subcommittee on Investigations to highlight an obvious gap in our border security. The U.S. Border Patrol is the uniformed law enforcement arm of the Immigration and Naturalization Service (INS) with the responsibility of combating alien snuggling and illegal entries other than at ports of entry. The Subcommittee looked at how people who attempt to enter the country illegally at places other than the official ports of entry are arrested and processed by the Border Patrol. When persons are arrested by the Border Patrol, the large majority voluntarily returns to their country of origin, usually Mexico or Canada. The others, perhaps as many as one-third of those arrested on the Northern Border, are given a notice to appear at a removal hearing. The Border Patrol decides whether the person should be detained, released on bond or, as is often the case, released on his or her own recognizance while awaiting a hearing. This hearing can take several months to occur.

In FY 2001 at the Detroit Border Patrol Sector—which encompasses all of Michigan—the Border Patrol arrested more than 2,100 people. A significant percentage of these people were arrested while actually attempting to enter the U.S. illegally. Most of these 2,100 were voluntarily returned to their country of origin. However, more than one-third were given a notice to appear at a removal hearing. Reports

from Border Patrol agents indicate that the vast majority of the latter group were released on their own recognizance pending their hearing. The INS wasn't able to tell us how many of the persons arrested in this situation and released fail to show up for their scheduled hearing. However, by looking at related statistics and ballpark estimates, we estimated that the number is at least 40 percent and possibly as high as 90 percent.

The conclusion is inescapable: The vast majority of people arrested by the Border Patrol while attempting to enter the U.S. illegally who don't voluntarily return to their own country are released on their own recognizance. Most of those released don't show up for their removal hearing and little or no effort is made to find them.

As I said at my Subcommittee's hearing, this is a dysfunctional and absurd system that makes a mockery of our immigration laws. When we release persons into the county who are without an address, without ties, without any record of who they are, we're abdicating our responsibility to the larger community. This is a practice that has to stop. On November 13, I asked the INS and Border Patrol to report to me on the steps they plan to take to close these enforcement loopholes. If the response is unsatisfactory, I plan to introduce legislation to accomplish it.

There is much that needs to be done. Customs and INS officials shouldn't have to rely on temporary fixes—we need permanent workers and we need them now. We also need to find a way to compensate our local law enforcement volunteers and secure funds for technology. We should also consider performing reverse Customs inspections of vehicles entering tunnels and crossing bridges on the Northern Border. With the increased security risks to our nation's infrastructure in the post-September 11 climate, it seems obvious that inspecting vehicles for bombs or explosives AFTER they enter our tunnels or cross our bridges is illogical. To rectify this security vulnerability, we must work with our neighbors to establish a reverse inspection program to inspect vehicles before they have the chance to endanger or destroy important transportation infrastructure.

And finally, we need to make common sense changes to our law enforcement and immigration policies to ensure the safety of our people and the integrity of our laws. We are an open and generous country and we welcome persons from around the world who want to contribute their hard work to help build a better America. But we also have a duty to protect ourselves and our country from people who would do us harm.

Chairman LIEBERMAN. Thanks, Senator Levin. Thanks for your involvement in this. Because I know of the great interest in Michigan about this, I look forward to the questions you have raised, and to working with you on some responses.

Senator Hollings, thanks so much for being here.

TESTIMONY OF HON. ERNEST F. HOLLINGS, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Senator HOLLINGS. Thank you very, very much, Mr. Chairman and Senator Levin. I am grateful to the Committee for the chance to appear here.

Let me ask consent that my prepared statement be included in the record.

Chairman LIEBERMAN. Without objection.

Senator HOLLINGS. I will get right into the advance check. I, frankly, had not heard of that, the concept of pre-clearance of cargo in foreign ports. Let me say, Senator Bob Graham of Florida and I, as you indicated, Senator Levin, we have been at it 3 years. We started off really in looking into drugs and the drugs coming in in containers. We were not thinking of explosives and terrorism particularly at the time. President Clinton, at our behest, put in a study commission. The study commission, comprised of 17 Federal agencies, made its report. We put in a bill in the last Congress with no further success. We have one in in this Congress that has been reported out of committee unanimously. And yes, we have been working to advance that bill forward as well.

Along that line, the only reason for the hold-up on the floor is OMB. Our Republican colleagues embarrassedly have to stand up and object on account of costs. You can ship a container anywhere into the United States for $5,000, and bring in explosives or chemical weapons. We had one terrorist that was picked up in Italy in a marine container, he had a phone, a toilet, cooking and sleeping equipment, and plans and security passes for some of the airports, false documentation to get into any and every entry point into the United States and everything like that. He was living in the container.

So either one can come in for $5,000, or you can get in the contraband needed to destroy our Nation. We have spent billions for the threats from outer space and a ballastic missile defense system but we do not want to spend port security. We know the cost of everything and the value of nothing.

This is an emergency situation. Let me, if the Committee will please, read from an article in the *London Times* entitled, "Secret Fleet Supplied Bombers," published over a month ago. "Three years ago, nobody paid much attention to a crew unloading a cargo from a rusting freighter tied up on the K-side at Mubasa, Kenya. The freighter was part of bin Laden's merchant fleet and the crew was delivering supplies by the team of suicide bombers who weeks later would blow up the U.S. embassies in Kenya and Tanzania. Bin Laden's covert shipping interests were revealed at the trial of the bombers, but until now, security services have been slow to track down how many vessels he operates."

Well, we have tracked it down now and he operates over 20 vessels, but he could easily hijack an oil tanker he does not own. Some company like Chevron, Exxon, or responsible owner's tanker could be hijacked and used as a weapon. You can operate one with four suicidalists, or martyrs, and run it right into the Golden Gate Bridge or the Brooklyn Bridge or any place in the United States.

So we are into an emergency situation and we have to go to the 50 largest ports, at least, and very quickly. There are some 361 ports, and let me join in, in support of the very comprehensive opening statement made by the distinguished Chairman. He has covered the subject. We have 361 ports, we have 50 major ports, and we have got to really move forward as fast as we can to have a plan of security there. Currently we don't have Federal security plans.

I think the big problem is that the whole thrust in port operations, and I used to operate one when I was a Governor and have been a big supporter of port facilities and economic expansion and everything else of that kind, but they are many splendored things. Some are owned privately. We are getting one privately developed right now in the State of South Carolina. Some are owned by the State itself. We have a State Ports Authority, and some are owned by the State Ports Authority but are leased out. For instance, the largest carrier in New York, Maersk lines, leases major portions of the port. Also associated in the operations of ports are the Customs Service, the Immigration Service, the Drug Enforcement Administration, the local police, the Coast Guard, and everything else.

To show you the lack of attention we did have, and it was not Admiral Loy, the Commandant, but another admiral was before

our committee just 3 weeks ago and we asked who was in charge of security at the port. He said he did not know. Under law, the Captain of the Port, namely the Coast Guard official, is really, under present law today, responsible for the security of the port, but it is joined in by the local FBI, DEA, all these other agencies that I mentioned.

And what we really need and the thrust of our bill is to get them all together and submit as judiciously and as expeditiously as possible a plan, to the Secretary of Transportation, a plan for security. They are all required to do that in the measure. There is some $1 billion overall provided with respect to quadrupling Customs agents and so forth at the port, buying the inspection equipment for the screeners. To my knowledge, the best screening equipment is down in Miami. That not only X-rays, but it scans the heat and can pick up drugs and articles in there. They tell me down in Georgia they are producing one that can even do better than that.

It requires the ocean shipping manifests of cargo coming in, but as I indicated, you can have a good check-off on an oil tanker, but it can easily be hijacked and brought in, so there is still that threat that has got to be taken care of, and we need maritime protection and to establish greater controls of foreign vessels.

I would be glad to try to respond to any questions. We have to get this bill out, and Senator Bennett, I was just saying our Republican colleagues embarrassingly have to object to it. I know they are for port security, but OMB has got them putting up a hold.

Incidentally, Senator Levin, it also includes the truck traffic coming in and the rail security and other modes of transport. We are trying our best to prepare the New York and Baltimore tunnels and so forth. You are going to hear before we leave about Amtrak and the tunnels over here in Baltimore, particularly going into New York and Grand Central Station. Those kinds of things have got to be cared for, or we will have problems.

So we are trying our best to clear it, and pass the bill through the Senate, and ours was passed out totally bipartisan, unanimously from the committee, and I again, will be glad to try to respond to any questions you have.

Chairman LIEBERMAN. Thanks very much, Senator Hollings. So the bill is on the calendar now?

Senator HOLLINGS. Oh, yes. It has been on the floor twice now and asked for its consideration, but there has been objection and my best look-see at it has been at the behest of the Office of Management and Budget on the matter of cost. Like I said, you can get a container brought in that has 60,000 pounds and thousands and thousands of those containers come in each day, largely unchecked.

Incidentally, you cannot find out the ownership of those containers or the ship. I have been working on that as well. Some are owned by the Chinese, and we have got one port out on the West Coast operated by the Cosco, a Chinese government controlled company. Others are operated out of Hong Kong. Some are holding companies and everything else like that.

The biggest difficulty I am having at the moment on the safety side of the equation at seaports is where the poor truckers that come onto the port facilities there and they spend 2 hours trying to get a safe container chassis, because nobody maintains the chas-

sis. If they get an unsafe one that blows a tire, or has defective lights, the patrolman pulls them over and they have lost their livelihood because they have gotten a fine and penalties to their driver's license, and the poor truck driver trying to work around the clock to feed his family has lost out. So he has to come there 2 hours early on the lot at the port itself trying to find something safe, and we have been trying to get some kind of requirements and everything at the port itself to check these things out. But, ultimately, the maritime business operates under a cloak of secrecy.

There are all kinds of problems, but the biggest is security, and there is no idea of security. The whole idea is, move it. If we can move it faster than New York can or some other port can, brother, we are going to get the business.

Chairman LIEBERMAN. So we have a very efficient but insecure system now at ports?

Senator HOLLINGS. Yes, sir.

Chairman LIEBERMAN. Is there money for port security in the $7.5 billion homeland security component of the DOD appropriations?

Senator HOLLINGS. The amount that is in that homeland security is only $50 million, but that will give us a good start to do the planning.

Chairman LIEBERMAN. A beginning.

Senator HOLLINGS. Yes, sir.

Chairman LIEBERMAN. I wonder, before Senator Hollings leaves, do any of my colleagues have a question?

Senator LEVIN. Thank you.

Chairman LIEBERMAN. Senator Hollings, thanks very much. We look forward to working with you.

Senator HOLLINGS. I thank the Committee very, very much.

Chairman LIEBERMAN. We will share the results of our hearing today with you, and once again, we thank you for your leadership.

Senator HOLLINGS. Yes, sir.

Chairman LIEBERMAN. Do either of my colleagues have an opening statement, Senator Bennett or Senator Torricelli?

Senator BENNETT. No thank you.

Chairman LIEBERMAN. Let us go to the first panel, then, and I am going to call Commander Stephen Flynn of the U.S. Coast Guard, who is now a Senior Fellow of National Security Studies at the Council on Foreign Relations, to go first.

In a very real sense, although I suppose we would have eventually found our way to port security as a result of this series of hearings, Steve Flynn's testimony before this Committee on the subject of homeland security really educated and alarmed us, and I think he has become something, at least in my mind, of the Paul Revere of 21st Century port security. So I do not want to work out whether the terrorists are coming, but they will come unless we raise our guard at the ports.

So I am going to give you a little more time than the 5 minutes because I know you have a presentation. I think it may frame a lot of the rest of the hearing. Go right ahead.

TESTIMONY OF STEPHEN E. FLYNN,[1] PH.D., SENIOR FELLOW, COUNCIL ON FOREIGN RELATIONS AND COMMANDER, U.S. COAST GUARD

Mr. FLYNN. Thank you very much, Mr. Chairman. It is a real honor to be back in front of you again today to talk about this very, very serious issue, and I certainly commend you, sir, for hosting these hearings, because at the end of the day, I think we are talking about not just trying to protect the American people from potentially another catastrophic terrorism event, but we are also talking here, as well, about the sustainability of global commerce, because how the terrorists do their work may force us to respond in a way that could sacrifice the movements of peoples and goods that are so essential for us to continue to prosper.

We saw that in the week immediately following September 11, when the United States had to do what no Nation could do to it, which was essentially to impose a blockade on its own economy. What we did was not just ground our aircraft, but we closed most of our major seaports and effectively sealed our borders with Canada and Mexico, and we did that because we did not have much confidence that we had the capacity to filter bad from good in all those flows coming our way.

We started the engine back up again and we have done a good scrubbing on the aviation side, but in my view, the aviation sector is the virtual Fort Knox of security by comparison to the other two sectors. The maritime and surface sector continue to be extraordinarily vulnerable, and we really have not come to grips with those issues.

I would like to talk a little bit about that, because I think what we have to take is another lesson from the September 11 time frame, is what we saw here is not a singular event by a single crazed individual or a network of individuals. I believe, as I think some others in the national security field, which I am a part, believe that what we witnessed on September 11 was really how warfare will be conducted in the 21st Century. What this means is that at the end of the day, regardless of what goes on in Afghanistan now, and it looks to be a very successful campaign, is that, essentially, we are only defeating the terrorists of the moment.

The United States may be an unrivaled power in terms of global military and economic and cultural reach, but the fact of the matter is, there are limits to that power. There will always be corners of the world for terrorists to hide in or failed states or failing states that have corners in their rural countrysides or mega-cities.

So we have to begin with the assumption here that there will be for the foreseeable future anti-American terrorists with global reach; that, second, they will continue, because of the age we are in, to have access to weapons, including chemical and biological, that could lead to a catastrophic terrorist attack here on U.S. soil; and we also have to conclude that terrorists and our adversaries who cannot take us on frontally in a conventional way because they will lose in that enterprise, that are thinking about attacking America asymmetrically, whatever their mode may be, will be in-

[1] The prepared statement of Mr. Flynn with an attachment appears in the Appendix on page 57.

spired by what happened by September 11, inspired because these folks made it look easy, and equally inspired and more soberly, perhaps, by the amount of particular economic disruption they have caused as a result of that single attack.

We have to realize at the end of the day that terrorism is not about just killing people or toppling buildings. There is military utility to engaging in a terrorist act if you can generate societal and economic disruption that weakens the power of your adversary and forces it to change its behavior. That is why, militarily, you would decide to engage in an attack in the way that we saw on September 11, or what I worry about, alternatively, potentially exploit or target our other very open and vulnerable systems.

What we saw on September 11, I believe, is the exposure of the soft underbelly of globalization. That is the very thing that has made America so successful and prosperous, our global reach and the networks that feed energy and labor and transport goods and people. It is also a system that remains extremely vulnerable.

The best way, I think, to illustrate that problem, and not just in our ports but in the broader issue, and I think this is the important point, I guess, I hope to leave, is that we cannot think about our transportation sector in isolated nodes. Unfortunately, our government is constructed that way. We look at surface, aviation, rail, and we divide it up and we often make these modes compete with one another for resources. The fact is, it is a network that allows for global commerce to move and global travel to move and it is almost interoperable in today's world. We call that intermodal.

The best way to illustrate, though, our current security measures, I would argue, is by taking a look at the container problem that you have mentioned this morning, Mr. Chairman. Let me try to illustrate it a little bit more.

Of course, we are talking about these 20-foot, 40-foot boxes that are so ubiquitous I think so few of us pay any attention to them. They are hurtling down the highways. They are on rails. They are on ships. We drive by them. But we think things so often that show up in Wal-Mart just magically appear there from a back room. They, of course, come from all corners of the world and they come to us via those containers. We are talking about, in 1999, they represented about 80 percent of all general cargo, but today, the numbers look to be well over 90 percent of general cargo that comes into the United States transoceanic comes in a container.

[A slide presentation was shown.][1]

Mr. FLYNN. Now, a little over a year ago, I had written in foreign affairs and I brought this up here as a way to illustrate this, a scenario where I put this man's face up and I said, if I had been a consultant to bin Laden, he had done this little job on one of our embassies, but instead, what he might alternatively want to do, as I suggested, is to buy a company that had been moving ceramics in the New York area for the last 30 years and then load that out of the port of Karachi and the container would perhaps move on, like you see these throughout the Asia area here, one of these con-

[1] Copies of the slide presentation by Mr. Flynn entitled "Bolstering the Maritime Weak Link," appears in the Appendix on page 80.

tainer movement operations, just from a barge that gets on one of these rusty freighters.

And we bring it to a place like Hong Kong. This is just one of five major terminals in the Port of Hong Kong. It is getting almost cartoon-like as you see the numbers. We are talking about 1.1 million container movements a month in the Port of Hong Kong. They are going to be loaded on something like perhaps the Virginia Maersk. This is a 6,600 TEU. If you can imagine, that is right there 3,300 railroad cars, 3,300 18-wheelers that are sitting not just on top there, but in the hull of that ship. That could be loaded in under 30 hours in Hong Kong.

And it would steam for Long Beach, perhaps, and then, because it is going to Newark, it would probably travel in bond. That means we would unload it right from the pier and it would go onto a rail car, like this, and it would head into the inland of the United States. Our Customs inspection system is built to inspect—it is confusingly called the port of entry, but it is basically the point where it enters the economy, which in this case would be Newark. So it would be the Customs inspector in Newark who would actually have responsibility to examine the manifest and to ultimately look at the container when it got to Newark.

Chairman LIEBERMAN. And that would be the first American to do so?

Mr. FLYNN. That is right. It would go directly from the ship. Customs could, if alerted, stop it, of course, in the port of arrival, but the routine is to allow it to move directly in and move it. And so it may travel through a place like Chicago. I have—you do actually see passenger freight, on that bridge there coming through is one. If I had a chemical weapon with a GPS transponder on it, I could set off that device. And what I would have done is, before anybody knows what is in the container and where it is from, I would have caused, obviously, a real catastrophic event near a major population center where—and this is a major rail hub, of course, near the airport, and that would be very disruptive.

Now, let us imagine we just had some of that, even on a smaller scale, and it led America to ask the question, how do we know what is in these boxes? And I think most people would be rather mortified to realize that we do not really have real command on that. There are upwards of 500,000 entities out there that can load boxes around the world. There are 40,000 freight forwarders that load the box, seal it with a plastic seal, typically with a number on it, and then it is off to the races. It goes from any where in the way I just illustrated onto a ship and is coming here. And then the verification is a Customs function done again at the port of entry.

Now, we would then say, well, gee, if we do the inspection at the port of entry, what happens if there was a bomb in there that was triggered when you opened it up? If we take—and this, by the way, is sort of a rail yard. It gives you just a sense of what we are talking about trying to manage and sift through.

But let us take the Port of Newark, for instance, and Admiral Larrabee will talk a little bit more directly about this here. This is the biggest container port, of course, on the East Coast, but this, I think, is a very important picture for us to realize what we are talking about.

Let me step up perhaps and point out, these are the container terminals here. This is an aerial view of Newark International Airport. I call this an intermodal moment. In a mile, you have container ships coming in off-loading. This is actually one of the major rail hubs that spiders off to the Northeast and the rest of the continent, along with the New Jersey Turnpike, along with the Newark International Airport. So we inspect the container in Newark and it turns out to be a bomb. Where is the plume going to go? I think we could imagine where it could go.

Out of that would be, I think most folks would suggest, let us not open the box and inspect it in Newark anymore. We do not want any uninspected boxes coming in. So, therefore, I guess we do not have any boxes coming into Newark. Forty-million people within 200 miles would have a very disrupted market as a result.

So I lay that out as a sense of what we are talking about is not just simply that we have a vulnerability and that somebody could bring something in and cause disruption, but really, this is again about the sustainability of global commerce. How we respond and are set up to respond to this threat could, in fact, itself have real ripple effects.

Out of those scenarios, I think there are three key things that we have to have in regard to the hearing today. First is that seaports cannot be separated from the international transport system to which they belong. Ports are really just, in essence, nodes in a network where cargo is loaded or unloaded from one mode, a ship, into other modes—trucks, trains, and on occasion, planes. Therefore, seaport security must always be pursued against the context of transportation security, and this has been very difficult because we have been taking this rather balloon effect approach to it.

Second, the port security initiatives must be harmonized within a regional and international context. One of the major ports for the Northeast is Montreal and Halifax. They bring in about a million containers between the two of them, half of which come into the United States. If you only regulated ports inside the United States, you may push some of these problems offshore into Canada, Bahamas, Vancouver, or even into Mexican ports that could come online here. So we have to be talking about this network not just within the U.S. domestic context, but also overseas.

Finally, since U.S. ports themselves are perhaps America's most critical infrastructure, they should not be viewed as the primary line of defense in an effort to protect the U.S. homeland. They are essentially the last line of defense.

Now, the fact that seaport security must be considered within the broader transportation logistic context that includes ports outside U.S. jurisdictions has obvious implications for how the U.S. Government is organized to safeguard them. First, I would argue we have three major structural impediments.

One is that the agencies with responsibilities for a specific transportation mode rarely communicate with their counterparts in the other modes. In fact, there is a pervasive culture of competition among the modes, often reinforced by the Congressional advocates, I think most rather dramatically illustrated just this last couple of weeks, when the House has decided to bankroll additional airport security by taking $60 million out of the supplemental monies

promised the U.S. Coast Guard to pay for port security. It's a little bit, from my view, here of the classic horse leaving the barn and closing the gate afterwards on that one.

The security challenge associated with seaports is not just one posed by conveyances, ships, but the operators, passengers, and cargoes on those ships. So we have a complicated problem of we have to get a handle on people, we have got to get a handle on conveyances, and we have got to get a handle on goods. But people is an issue of consular affairs. That is State and INS. Goods are U.S. Customs, USDA, and FDA. Ships and the non-land side of the ports are Coast Guard, but the land side is a smorgasbord, depending on what port you are here, of local, State, and private entities. And then there are the trucks. About 10,000 trucks come into the Port of Newark each day, entirely unregulated activity.

And then, finally, since the jurisdiction of most of these agencies runs out at the water's edge, they tend to approach the regulatory enforcement issue with some strictly domestic contest or framework, rather, than an international one, and the international security community pays no attention to this problem.

So that is the state of affairs we are in, in a very quick framework, as I think many of the witnesses can fill in the blanks. But I think the key here, I hope that this illustration provided highlights the importance of not thinking that we can achieve homeland security in this regard at home. We have to be looking at this as a network and for what it is, which is one that moves overseas.

Our ultimate objective should be, go to the point of origin, and how we get to this is, I think, first, with some standards about how one gets to load a container, who gets to load it, and the process that is done. It has to be done in a sanitized way. Standards have to be identified in that and pushed through, whether it is the International Maritime Organization or the World Customs Organization, to say, if you stuff a box and you want to be off to the races to come to a port in the United States or in any of the other large ports in the world, you have to meet some basic requirements, and if you cannot do it there and we cannot feel comfortable with that, you have to restuff the box at a place that we feel comfortable that we know what is there and that there is a trusted partner who is doing that loading.

Second, when it is loaded, we want you to track it. We want you to know where it is. This is sort of what I call in-transit visibility and accountability, using technologies like GPS and electronic transponders and so forth. As soon as it leaves the factory, it goes from there to the terminal and we can account for it every step of the way.

There are two purposes for in-transit accountability and visibility. One is ideally to deter it. There is not much time for a bad person to bring something in. But most importantly, as well, is that when you have intelligence that there may be a compromise, which is perhaps the only way we are going to find, in many instances, a problem, it becomes actionable intelligence, that you can pinpoint immediately where the problem is and go in and, working with the carrier, you will be able to identify and figure out where the best way to manage that compromise might be.

Then the terminal operator itself would have to have accountability of the box. That happens as a matter of routine in most places. And then the ship mills where it is, and then the same on the receiving end when it is loaded off, and in the case of in bond shipment, again at trails along the way.

Then we have this complete control, sanitized control, and if that is done with the technologies and the cooperation—and the final piece is sharing data about who and what you are up front to allow agencies to assess that against any watch list they may have—if you do those three things, security up front, in-transit visibility and accountability, and the sharing of data, you get the easy trade lane. We are going to move you quickly, which makes sense from a security standpoint, because goods that rest often are most vulnerable to crime. So you actually have a security incentive, not only a market one, to accelerate if you can be confident up front.

That is why I am confident this is going to be workable if we think in these terms, because we can really—it has always been a false proposition in my view, openness versus control. Without control, the whole system is in jeopardy. That is what we saw on September 11. With smart controls, there actually is a national security rationale to fix things that have been broken for a long time, agencies that have paperwork requirements that make no sense or that are duplicative and redundant, bottlenecks in infrastructure that should not be there. We need to fix that from a security standpoint, and that, I think, parades an opening for this to be dealt with, not just here at home, but also overseas.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Dr. Flynn, thank you for an excellent opening statement. The country is fortunate that you have had the practical and academic experience you have had and you have brought them together at a time when, post-September 11, we need that very much, so I look forward to questioning you.

I am pleased to say Senator Collins is sitting today as the Ranking Republican Member of the Committee, and I think it is appropriate that I ask her now if she would like to make an opening statement before we go on to the other witnesses.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you very much, Mr. Chairman. I apologize for being a few minutes late for the hearing.

I want to thank you for convening this important hearing. Coming from the State of Maine, as I do, the vulnerability of our ports is of particular interest and importance. Our seaports are as important in the war against terrorism as the safety of the food we eat and the security of the planes we fly in. With more than 95 percent of our imports flowing through our ports and with millions of passengers and maritime containers passing through them with only limited inspections, we must have a far better security system in place than we do now.

Correspondence that I recently received from Captain Jeffrey Monroe, the Director of Ports and Transportation for Portland, Maine, makes the need for better port security very clear. Captain Monroe, in commenting on the security of our ports, put it bluntly. "Our local, State, and Federal agencies were, in many cases, ill pre-

pared for September 11 and the coordination of information and effort was almost nonexistent," he wrote. Captain Monroe's letter includes a series of specific recommendations and I would ask that this correspondence be made part of the record.[1]

Chairman LIEBERMAN. Without objection.

Senator COLLINS. Since September 11, the Coast Guard has expanded its patrols in Portland's harbor and has increased its surveillance of ships entering the port. But given the volume and the lack of personnel, this is a daunting and exhausting task. We must improve coordination between Federal, State, and local agencies, as well as the private sector. We must have highly trained and a sufficient number of employees. We must have a clear chain of accountability to achieve port security.

It is evident that we have a great deal to do and I am very pleased that the Chairman has assembled such a distinguished list of witnesses to assist us in this goal today. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins. I really look forward to working with you on this. I think this is an area where the Committee together can make an important contribution and I thank you for that excellent opening statement.

The next witness is Amanda DeBusk, now with Miller and Chevalier, former Assistant Secretary of Commerce, former Commissioner, Interagency Commission on Crime and Security in U.S. Seaports. Thanks so much for being here.

TESTIMONY OF F. AMANDA DeBUSK,[1] MILLER AND CHEVALIER, FORMER ASSISTANT SECRETARY OF THE COMMERCE DEPARTMENT AND FORMER COMMISSIONER, INTERAGENCY COMMISSION ON CRIME AND SECURITY IN U.S. SEAPORTS

Ms. DEBUSK. Thank you very much. I am honored to be here today. I am speaking to you as a former Commissioner on the Interagency Commission on Crime and Security in U.S. Seaports. President Clinton established the Commission by executive order on April 27, 1999. Senator Bob Graham was particularly instrumental in the Commission's establishment. I served on the Commission as the Commerce Department representative in my capacity as Assistant Secretary for Export Enforcement. The Commission issued a report in August 2000 with 20 findings and recommendations. I would like to highlight those that are most important for this Committee post-September 11.

Let me provide some background. One of the underlying concerns was how wide open our seaports are compared to our airports. In most cases, there is free access to the seaports. The Commission found that significant criminal activity was taking place at most of the 12 seaports that we surveyed. At many seaports, it is legal to carry firearms, so criminals with arms may have access to terminals where passengers embark for cruises.

Concerning cargo, because of misreporting and lack of reporting, no one knows in a timely fashion, if ever, what is in those containers at our seaports. One of the cases my former office inves-

[1] The letter from Captain Monroe with an attachment submitted by Senator Collins appears in the Appendix on page 142.

[1] The prepared statement of Ms. DeBusk appears in the Appendix on page 93.

tigated involved a riot control vehicle that was exported to China as a fire truck. The vehicle, it was a huge thing. It resembled a tank. It had a turret on top for spraying pepper gas all around. It was all boxed up in a container and at the time of export, no one knew what was inside the container and so it was exported as a fire truck.

The Commission approached the crime and security problem with the possibility of terrorist activity associated with the new millennium. Thankfully, nothing happened.

At that time, the FBI considered the threat of terrorism directed at any U.S. seaport to be low. However, even though the threat was low, the FBI considered that our vulnerability to attack was high. The Commission found that the state of security at seaports generally ranged from poor to fair, with a few exceptions where security was good.

We looked at fundamental activities for combatting terrorism, protective measures, crisis management, and consequence management. These activities require comprehensive interagency coordination. They involve law enforcement, intelligence agencies, emergency response agencies, and if needed, the military. Outside the Federal context, coordination is needed with the State and local authorities and the private sector.

Today, I would like to highlight recommendations in four areas relevant to this Committee: Enhanced interagency coordination, physical security at the ports, better and more timely information about cargo transiting the ports, and increased use of technology.

First, we need better interagency coordination. There are 361 seaports. Most ports are chartered by States or local government. Some terminals are operated by public port authorities. Others are private. There is no central Federal authority. There are at least 15 Federal agencies with jurisdiction at the seaports. In addition, there are State and local agencies and the private sector. Every single group is important for combatting terrorism and has something to contribute, but coordinating these groups is a monumental undertaking. Perhaps a Department of National Homeland Security could play a leadership role in this coordination.

The Commission found that there needed to be a comprehensive and definitive statement of Federal responsibility. The Federal Government needs to conduct threat assessments to determine where the threat is greatest and where we urgently need preventive measures. The Federal Government should strengthen coordination to more effectively address terrorism. It should work with all stakeholders. Key information available to the Federal Government should be disseminated to others, as needed.

Let me provide an example of where better coordination would be useful. The FBI has excellent regional counterterrorism task forces that consist of Federal, State, and local agencies. However, at the time of our study, these groups did not focus on the seaports. They should do so.

S. 1214, an amendment to the Merchant Marine Act, has some good proposals on establishing local port security committees.

Second, the Commission found that we need better physical security at the seaports for both vehicles and people. At many ports, access is virtually uncontrolled. At one of the ports I visited, we saw

a line of vehicles that was parked right beside the vessel. We were told that these were the dock workers' vehicles that were parked there for convenience. At the time, and as Senator Hollings alluded to, we were trying to figure out if this is someplace where drugs could be hidden for things coming off of vehicles, or coming out of containers and being stashed into the vehicles. But now what we have to do is think about the possibility that these vehicles lined up right beside the vessels might contain a car bomb or even a "dirty nuclear weapon" that could be hidden inside them.

Many ports do not have ID cards for personnel. I observed all sorts of people that were milling around at dockside. There was no way we could tell who should be there and who should not. The Commission found that at one point, pedestrians could freely walk through the purported access control points without even being questioned. We did not even want to contemplate a group of terrorists taking over a cruise ship, but it is a possibility.

Training of security personnel is also a problem. Many seaports use private security personnel who lack crime prevention and enforcement training.

The Commission recommended developing regulations to create a secure area where passengers board and disembark vessels. We also recommended proceeding with an INS project to manage risk with respect to both passengers and crew. We recommended creating shared dockside inspection facilities so that all relevant agencies have ready access to conduct inspections. The Commission called for the establishment of minimum guidelines for physical security, such as fences, lights, gates, restrictions on vehicle access, restrictions on carrying firearms, the establishment of a credentialing process so you would know who is supposed to be there, considering criminal background checks for those with access to sensitive areas of the port, and development of a private security officer certification program. S. 1214 moves in the direction of these recommendations, but it does so through voluntary security guidance. The Committee should consider making some of those requirements mandatory.

Third, we need better information about cargo transiting the ports. On the import side, information is often vague and import entries may be filed 5 days after arrival. On the export side, information tends to be very general, with descriptions like "general merchandise" that really do not tell you anything, and is required 10 days after export. One of the concerns with providing earlier and more detailed information is that it would allow specific cargo to be targeted for theft by those with access to the information, and this concern needs to be addressed.

Fourth, we need better technology at the seaports. Better technology is needed for a whole variety of applications, which include X-raying containers, using computer systems to target cargo associated with high-terrorist risk, collecting data on crimes at seaports, and providing real-time information for tracking high-risk cargo and personnel.

In sum, the Commission said, "A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property, and business, affect the operations of harbors and the transportation infrastructure, in-

cluding bridges, railroads, and highways, and cause extensive environmental damage." We need to take action now to reduce the risk of future catastrophes.

Thank you for inviting me here today to testify on this important subject.

Chairman LIEBERMAN. Thank you, Ms. DeBusk, for excellent testimony, which, unfortunately, continues to paint a harrowing picture as I listen to it.

Rob Quartel is our next witness. He is the CEO and Chairman of FreightDesk Technologies and a former member of the U.S. Federal Maritime Commission. Thanks for being here.

TESTIMONY OF ROB QUARTEL,[1] CHAIRMAN AND CHIEF EXECUTIVE OFFICER, FREIGHTDESK TECHNOLOGIES AND FORMER MEMBER, U.S. FEDERAL MARITIME COMMISSION

Mr. QUARTEL. Thank you, Senator. The last time I think I saw you up close was about 6 or 8 months ago at Sutton Place Gourmet, and I cannot remember what you were buying—— [Laughter.]

But I would observe that probably half of what you and I bought came in on a container. The meat probably came from Australia. The flowers and other vegetables probably came from Latin America, and so on and so forth, so this is a problem that is right here, wherever you are, every day. You are standing there in the middle of the system. It is probably a good thing you cannot remember what I was buying.

Chairman LIEBERMAN. I certainly cannot remember what I was buying.

Mr. QUARTEL. I know that what I was buying was something fattening.

Chairman LIEBERMAN. Senator Collins and I were saying, I wish I could say it was all American, but I am sure it was not. [Laughter.]

Mr. QUARTEL. But that is the beauty of the system——

Chairman LIEBERMAN. Yes.

Mr. QUARTEL [continuing]. The fact that we are able to access all these markets worldwide, whether they are food, whether they are the subcomponents of manufacturing. That is really what makes us efficient as a country and contributes to the national economy.

I would like to thank you for the invitation. I have got a quick slide show, and because of the time, what I am going to do is kind of truncate some of this and really kind of talk to the slides.

But I think based on Commander Flynn's and Ms. DeBusk's statements, this is really a scary issue and I would like to make one point of policy that I think the Committee ought to adopt, which is very straightforward. Every container destined to either land in or go through the United States, and the last point is really important, in my mind should be treated as a potential weapon of mass destruction, every ship that carries it as a delivery device, and every port as a potential target, and that suggests several things.

[1] The prepared statement of Mr. Quartel with attachments appears in the Appendix on page 98.

First, it suggests you cannot let a terrorist container get into the port. The port is the target. You saw the map where you had everything within a mile there in the Port of Newark, which, by the way, is what makes that a very efficient port, because you can switch from mode to mode to mode, whatever happens to be the most efficient way to do it.

It also suggests you cannot let it on a ship, and so one of the concepts I would like to talk to today is the notion of pushing the border back electronically. Ms. DeBusk talked about the fact that we collect a lot of data. Every part of the process is documented. This slide I am going to talk to in a minute shows the complexity of it, but you need to bear in mind that everything in the process is documented.

From the time it is purchased, a buyer or seller transaction creates a purchase order that says what it is, how many you want, the weights, eventually all the rest of that, to the trucker who picks it up, to the train who moves it, to the ship that carries it, to the train that delivers it, or truck in the United States, all of that is documented in a series of documents. What does not happen, as Ms. DeBusk said, is that it does not all get there to Customs or anyone else early. It gets there strung out across the process.

[A slide presentation was shown.][1]

Mr. QUARTEL. This first slide really is intended to talk to the issue of complexity. The international trade process is hugely complex. It is not like domestic trade, which goes from point to point. You have in every single trade 20 to 25 involved parties, whether they are the buyer, the seller, the transportation modes, all the rest of those. You have as many as 30 to 40 documents. You have a couple of hundred data elements. The messages all arrive in a variety of different kinds of platforms, some electronic, some fax, some by E-mail. But it is a tremendously complex process.

Admiral Loy has pioneered a concept called Maritime Domain Awareness, and I think that is very relevant to this port issue here.

By the way, I also would ascribe to what Commander Flynn said earlier. I view the port as really too late. In my mind, the port is the least of the problems. Yes, you have to protect the port. Yes, you have to protect the physical integrity of it. Yes, you have to have all the security measures. The real problem is at the beginning of the cargo. That is where you have to interdict it.

I would take Admiral Loy's thought and actually press it a little further. I really suggest that there are five domains in international trade. The first is the origin of the cargo. In manufacturing today, you might have a company that does virtual manufacturing in Asia, where they will have 20 different factories that are all subcomponents of the process. It starts in one. It moves by truck to another. It moves by truck to another, by train to another, and another to another to another, literally that many, and then is assembled in one place and forwarded to the United States. So that is part of the process that includes inland transportation, all of the parties engaged in manufacturing.

[1] Copies of the slide presentation appears in the Appendix on page 107.

The second, at the port of loading. And on this chart, by the way, one of the things I have done is just very quickly, and it is not necessarily 100 percent accurate, I did it on a plane in the middle of the night the other night, is to talk to some of the agencies on the issue of where some of their authorities might lie in the process, U.S. Government agencies, and also, as has been said earlier, these authorities tend to be sort of stovepiped. They are aimed at a specific part of the process. That is really all they can do under the law.

The second part of it is in transit. There are a number of protective things you need to do there.

One of the things from end to end, of course, is visibility. Companies are going to that, to tracking the cargo, though tracking is not nearly so pervasive as we seem to think it is, based on when we go to the web, we seem to know where everything is. One of the reasons is that much of what we think of as being tracked is in FedEx packages, typically air freight, which is different than ocean and land, which are in containers.

The fourth is the port of discharge, which is really, I think, the point of the hearing today.

And then finally, multiple destinations.

If you want to figure out what is happening to a cargo, you really need to know what it is, where it came from, where it is going to, who has touched it, what did they do with it, what did it cost, who paid for it, and that is all the kind of data that is collected in a system.

The information process itself provides an attraction because, if you work at it, you can hide the transaction. This really kind of talks to the issue of how cargo moves. Forty or more days before it gets here and just in time, you may have a buyer-seller transaction. They generate a letter of instruction and a commercial invoice.

On this slide, the red documents are reported to Customs. It goes to a warehouse. It finally gets to a ship and the ship creates a master bill of lading. A single container might contain as many as 10 or 20 different cargoes. It may be 10 containers which are the same shipments, they are all the same thing to the same manufacturer. Containers are not just packed by one person. They may be packed by multiple people. You have people at each end who consolidate what is in a container. You have people at the other end who deconsolidate it and send it off in a bunch of different directions.

Carriers generate documents. Throughout the process today, you typically have an intermediary, a freight forwarder or a customs broker or a third-party logistics provider. That, by the way, is one place that I think in the future we need to focus some of our thinking about how you manage the process for the government, because they are the ones who typically handle the paperwork as well as the financial documentation. You have additional carrier reporting at the end. And then, finally, you have another set of documents generated.

What I would like to suggest to you is today, we tend to think of the border at the bottom there as being the physical border where the ship comes in. The concept I would ask the Committee to consider is to push that border to the top of the page between

the warehouse and the port of embarkation and to do that electronically.

The next two slides—this is a sample of the kinds of data that comes out of the documents that are generated in a typical commercial transaction. By the way, when a ship lands in the United States, it drops off 40,000 documents.

Chairman LIEBERMAN. Forty thousand?

Mr. QUARTEL. Documents for 6,000 containers. So that is my 10 to 20 to 30 documents per container.

Chairman LIEBERMAN. And who gets those documents?

Mr. QUARTEL. Customs gets some of them. The shippers get some of them. Letters of instruction and financial letters go off to the people who handle that. So there is a lot of data. That is one of my key points to you. This is not a new process. Part of what we have to do and the opportunity here is to manage the data process, and we can talk to that.

If you go across this, you can get everything I am talking about. You can find out—and this is the other part of it, is another 60 different elements. You could find out who paid for it, what it is, what it weighed, where it was coming from, how it went, by truck on the way, on the way back, the ship. If you go to the ship, you can actually tell what was going with it side by side.

Now, the process I would like to suggest to you—I am going to go actually one slide further and then come back. The process I would like to throw at you for your consideration is a kind of profiling process. You create a commercial database from the kind of data which is currently provided by the commercial sector, some of which goes to the government and some of which does not, and some of which should not go to the government because it is essentially competitive data. But you can create a commercial database.

We already have a database and bases of government data. The Coast Guard, for example, has what is called a fusion center, where they fuse conceptually data from a variety of different kinds of law enforcement sources. Right now, that data is not always compared against each other and it is certainly not compared when a cargo originates.

What I would suggest to you is that you create a new process, perhaps driven by Customs, in which you collect the commercial data, you collect the law enforcement data, and you run it through a decision algorithm which basically says, well, what is wrong with this? Is it—and I can show you back here two slides—is the cargo something that is said to be coming from a place where it is not manufactured? Is it steel coming from Romania, where they do not have a steel factory? Is it coming from Afghanistan but going to the heart of New York? Is it something going by a nuclear power plant?

If you go through the documents, and this is just kind of an example of it, you can actually see where you can find these anomalies, and while I am not an expert in the mathematical profiling aspect, I do know a lot about the data management process. But there are people who are expert in profiling and we are dealing with some of those and I have been working with the National Defense University, which looked through some of this, who create the kinds of algorithms which can help you decide, and we use some of this today with drug enforcement, but not to this extent.

Chairman LIEBERMAN. Mr. Quartel, excuse me, but you have gone beyond the 5 minutes now——

Mr. QUARTEL. I am sorry. I am going to finish right now.

Chairman LIEBERMAN [continuing]. So if you can begin to think about wrapping up.

Mr. QUARTEL. I am done, virtually.

Chairman LIEBERMAN. That was good timing.

Mr. QUARTEL. Thank you.

Chairman LIEBERMAN. Thanks very much for very thoughtful and helpful testimony, which we will look forward to questioning you on.

Our final witness on this panel is Richard Larrabee, who is a retired Rear Admiral of the U.S. Coast Guard and now Director of the Port Commerce Department of the Port Authority of New York and New Jersey, so a person with great experience and right in the middle of the topic that we are discussing today. Thanks so much for being here.

TESTIMONY OF REAR ADMIRAL RICHARD M. LARRABEE,[1] RET., DIRECTOR, PORT COMMERCE DEPARTMENT, THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Rear Admiral LARRABEE. Mr. Chairman, thank you. Members of the Committee, good morning. Thank you for the opportunity to testify this morning.

I have provided written testimony and would ask that that would be placed in the record.

Chairman LIEBERMAN. It will.

Rear Admiral LARRABEE. What I would like to do is just take a couple of minutes in the interest of time to touch on some of the things that the prior testimony has talked about, but do it from a ports perspective.

Mr. Chairman, as you said before, the ports of this country are a vital intermodal link in our transportation system and a large part of our economy. The Port of New York handled about three million containers last year, about 560,000 automobiles, and over 30 billion gallons of petroleum products, the largest petroleum port in the United States. That system, as the Chairman suggested, is based on speed, reliability, and cost, and we are living in a "just in time" society where the movement of those goods are critical.

On the morning of September 11, the Port of New York and New Jersey was closed. It was closed by the Coast Guard captain of the port. Other law enforcement agencies were involved in that decision, but it was done in a very orderly way. There was a tendency in the port from one perspective to keep the port closed because of the fear of the threat of terrorism. On the other hand, the pressures that Commander Flynn talked about of keeping commerce moving were obviously part of that discussion.

Because petroleum resources were going low, because of a shortage of other supplies that would normally come through the port, we felt a great deal of pressure to open the port up as quickly as possible, and on the morning of Thursday the 13th, we reopened the port with a large number of security measures in place—all

[1] The prepared statement of Rear Admiral Larrabee appears in the Appendix on page 114.

ships boarded by the Coast Guard at sea, all manifests, both cargo and crew manifests, checked, tug escorts into the port, and an extensive cargo inspection program by both Customs and Coast Guard and other law enforcement agencies, a heightened level of activity in terms of spot checks and patrols in the port.

That level of activity, along with an extensive effort by the Coast Guard to protect vital assets of the Port of New York and New Jersey, certainly was an extraordinary effort on the part of all of those Federal agencies, but it simply was not sustainable, and today in the Port of New York, we are seeing far fewer resources doing those kinds of things when today the level of our security might have to be higher than it was perhaps the day after September 11.

I want to talk just briefly about this notion of who is in charge, because we certainly heard Senator Hollings talk about that. I think we have other models that we can look at. In my own experience, I can tell you that in the wake of Exxon Valdez, the U.S. Senate and the administration at the time certainly supported efforts to improve that system. The end result was OPA 1990, and since that time 10 years ago, we have seen a dramatic decrease in not only the number of spills and the size of spills, but an increase in our ability to respond. One of the key issues in that legislation was answering the question: Who is in charge?

As it was suggested this morning, I believe the Coast Guard Captain of the Port currently has the jurisdiction to do a number of things that we have heard about. Perhaps his position needs to be strengthened, but I believe the Coast Guard is in the right position to manage both the prevention and the response to an incident like the one we are talking about this morning.

We have heard an awful lot about this notion that perhaps the greatest threat in one of our ports is not a large tanker hitting one of our bridges but the entry of a weapon of mass destruction using our very efficient container movement system, and there is no question about that.

I believe that last week, Admiral Loy, the Commandant of the Coast Guard, addressed the Assembly of the International Maritime Organization and proposed that a working group be established to look at port security and terrorism, specifically at the issues of cargo visibility and accountability. We certainly support the Coast Guard's proposal and believe that the IMO is one of those appropriate forums to address the issues of international concern, and I think there certainly are parallels in this area, too.

The shipment of hazardous materials these days is a process that has seen dramatic improvements over the last 20 to 30 years. Today, the kinds of accountability and responsibility of moving those kinds of materials certainly gives us opportunities to look at parallels when it comes to moving other cargoes.

We have heard a little bit this morning about this notion that communications is the foundation of coordination, and certainly there is a real need to share intelligence and threat assessments among the Federal, State, and local agencies, and I would have to say to you this morning that as Director of the Port of New York and New Jersey, I am not in a very good position today to tell you whether our measures that are underway right now are adequate

for the threat that is out there. We simply are still not sharing the kind of threat assessments that I think need to be in place.

Chairman LIEBERMAN. That is a very important statement. Forgive me for interrupting, but I hope we all listened to it. That is an unacceptable situation. You just feel you are not getting the intelligence information you need?

Rear Admiral LARRABEE. As Senator Hollings said, this is a system that really is being managed day to day by the private industry, and it is not only the Port Authority, but more importantly, terminal operators and shipping lines which need to be brought into this circle and be made more aware of what the threats are and what they can be doing in a practical way.

I think there is a need for standards, and Senator Hollings talked about that this morning. My Port Authority Board is asking me what I should be doing and my answer to them is—I am waiting for Federal legislation. We desperately need to pass the Hollings bill in the very near future and I would ask you to support Senator Hollings' efforts.

Just to conclude my statement, this is a system that, as you have heard this morning, is the responsibility of an awful lot of people, whether it is the paperwork or the number of agencies involved or the number of hands that move this particular cargo. It simply is a system that requires the diligence and responsibility of an awful lot of people. We believe that there are ways to make the system more secure. We believe that we have to do that.

We are very appreciative of the kind of support that we have gotten from agencies like the Coast Guard, the FBI, and Customs, and we are very hopeful that you are going to be able to give them the kind of resources that they are going to need to do their job.

Finally, I want to thank Senator Torricelli and others for supporting us in the local New York area. Supplemental legislation has been passed, and I know, for one, we are going to be getting some extra resources in the port in order to improve our security level. Thank you.

Chairman LIEBERMAN. Thanks, Rear Admiral, for very helpful testimony from a particularly important perspective.

Let me focus in on this question of coordination. It is a fascinating and, in many ways, troubling picture, even from an organizational point of view. And again, as I said in my opening statement, when I got more into this, I was surprised to be reminded that there is no Federal coordinating role here, that the ports are State and locally overseen, that there is a lot of private interests involved. Ports in Connecticut, for instance, most of them are owned privately, the harbor facilities.

Give me a sense of what happens at a typical port, either privately owned, and/or locally regulated. Are there Federal agencies present at the major ports? Are they coordinating now? Maybe, Rear Admiral Larrabee, you could give me a picture of what is happening at a typical port of entry.

Rear Admiral LARRABEE. Well, I do not think there is any question that there is a great deal more coordination today than there was on September 10.

Chairman LIEBERMAN. Yes.

Rear Admiral LARRABEE. The boardings that I talked about that the Coast Guard is conducting, vessels are being boarded on a priority basis based on an analysis of that vessel and what sort of threat it might pose to the port 96 hours before the vessel arrives, and my understanding is that both Customs and the Coast Guard and INS are looking at cargo manifests and crew manifests, ports of destination, and making decisions about whether or not to board and what to look for. So that is there.

Chairman LIEBERMAN. Is that the universe we are talking about, Customs, Coast Guard, and INS, of Federal presence at the ports?

Rear Admiral LARRABEE. I think, for the most part, that covers all of the issues that we have talked about this morning.

Chairman LIEBERMAN. Let me then ask what can be done to either facilitate better communications between the front-line agencies in securing our ports, and more broadly, whether you think there is a need for active Congressional involvement here through legislation to create some kind of new overarching Federal organization to be concerned about the ports and to guarantee coordination. Ms. DeBusk.

Ms. DEBUSK. Yes. First to answer your question, I do think there is a very strong need to have an umbrella to coordinate all this, perhaps through homeland defense.

Let me just sort of give you a little vignette of what happens there. You have 15 Federal agencies with some sort of authority at the port, and——

Chairman LIEBERMAN. Fifteen, well beyond the three I mentioned.

Ms. DEBUSK. Absolutely.

Chairman LIEBERMAN. Just name a few more.

Ms. DEBUSK. You have the Commerce Department and you have the Agriculture Department, you have the Food and Drug Administration, you have all these, and let me just take a few of the older ones that you do not necessarily think about, like EPA, for instance.

Let us just take the Agriculture Department. They would perhaps know how to be on the lookout for contaminated food coming in. Let us just think about a terrorist who decides to sprinkle a little cyanide in all the Cheerios, right. They would know how to be on the lookout for that, but that is not the expertise of the Coast Guard.

In my former office, Export Enforcement, we knew how to target, to look for things that might be used for weapons of mass destruction or chemical or biological agents. But again, that is not the job of the Coast Guard. The Customs folks, they know how to look very well for the drugs that are coming in or going out. That is one of their specialties, and obviously the drug trade supports terrorism.

But again, no one is bringing all these pieces of the puzzle together and I think there is a strong need for perhaps the Office of Homeland Defense or some other body to be able to do that.

Chairman LIEBERMAN. Dr. Flynn, I know that you and Mr. Quartel are asking us to consider pushing the border back, a very interesting idea which I know the Committee will want to get to in a few moments. But what about the border where it is, even if you push it back? What do you suggest from your experience and

work as to what we should do, if anything, to facilitate better communications and coordination among the 15 Federal agencies and the State and locals and privates involved to guarantee a more secure and efficient situation?

Mr. FLYNN. Let me say, Senator, that while I am talking about pushing the border back, that we think about this problem as one that starts much farther away than our border. I am not calling for the end of the border.

Chairman LIEBERMAN. Right.

Mr. FLYNN. That is, it is really a series of concentric circles that to the best of our ability, we put the most intensity at the origin point and then the number of inspections narrows down as we have to get to our own entry because of the volume and velocity issue that we face here.

What is clear is that we need a general pool of data, and there was an effort that Customs was involved with in the former administration to create what was called the International Trade Data System that would bring all the kinds of things that Mr. Quartel outlined there all in one pool and allow the agencies to shop within that data.

Most of what we find is things also, as Mr. Quartel talked about here, is this anomaly detection, the things that do not make sense, a high-value good going on a slow boat to China originating from a place, as he said, that does not make steel. And so what you need there is this data up front and you need it in a pool, and ideally you also would be housing people together.

We have models for this in the drug world. We have the EPICs, the El Paso Intelligence Center. We have similar efforts in Jonestown and so forth here. But what we have learned here is that just to try to take that small segment of high-risk drugs, we really have to now think about all general cargo as at risk, as it always has been, and it is not just for narcotics, of course. Now it is human trafficking, but especially this concern with weapons of mass destruction. So there are various useful models of how we bring data and infuse it that is brought out of the drug world. We just need to expand, in part, upon that.

But we rushed with some legislation here right after September 11 to put more primary inspectors. You look at everything, you see nothing in this business, and we all know this from those people with the glazed eyes who look at the X-ray machines as the luggage goes by. That is not the way to do it. You have to be smarter.

And so the challenge here is analysts, well-trained people who know their segments and markets—and this issue of information sharing is huge. I am almost confident, for instance, that Rear Admiral Larrabee has not been given a clearance and it would probably take him about a year or two, perhaps, to get a security clearance. He was a former flag officer in the U.S. Coast Guard that has been doing this for years and we cannot find a way to clear him into a system to share intelligence that would be useful for him as a decision maker and a manager at work here. These stovepipes are huge and have to be addressed.

Chairman LIEBERMAN. Well said. My time is up. Do you have a clearance?

Rear Admiral LARRABEE. No, sir. I had a clearance, but I have not gotten it back yet.

Chairman LIEBERMAN. Yes. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Commander Flynn, I understand from my staff that through discussions that they have had with Rear Admiral Naccara that you have been involved in developing a Northern New England Border security project. Could you tell me about that project and whether you think it would help solve some of the coordination and communication problems that we have heard about today?

Mr. FLYNN. Sure. This is actually spawned out of the State of New Hampshire, and Governor Jeanne Shaheen actually took a real leadership role and interest on this.

This is obviously a real concern by most of the Northern States, and Senator Levin was here as well, about the hardened border and what that would mean. In the New England context and Northern New England context, this is about the Port of Montreal and Halifax, as well. About half the containers coming to Halifax and Montreal come into the United States. So getting a handle on the cross-border trade is central without a kind of hardened, sealed border approach.

The notion here is that I was very excited to hear in terms of this interest in New England, and I think it is something that we need as a model overall. We have to do some experimentation, and I think the way this is done is some delegation by the headquarters here to regional commanders, such as Rear Admiral Naccara and the Regional Director of Customs and let them work with the governors and private sector, trusted partners, and with their counterparts across the border in the provinces and the ports in Halifax and begin to do this process of vetting legitimate players and finding ways to expedite their movements, applying some of these technologies.

Ideally, we will find some companies up there who will want to play. There will be some resources found to test some technologies and you bring together INS, Coast Guard, and the other players, FDA and so forth, to try to get a handle on this.

So what there seems to be, I know she has contacted Governor King in Maine and Governor Dean in Vermont and there is interest, I think, in Massachusetts, and I have been up in Ottawa last week, in fact, testified before their House of Commons on this issue. There is real interest on the other side of the border to try to come to arrangements where—this, I think, is so important. What we are trying to do here is not just find the needle in the haystack bad thing. What we are trying to do, as well, is to take the legitimate trade and travel and validate it as such we can set that haystack aside. That way, even if we had something as horrific as happened on September 11, we do not have to stop that flow. We know what it is. We do not have to stop those people, stop that train.

And so part of our efforts should be not entirely driven towards finding that one needle, but it should be focused on how to take the vast majority of legitimate goods, validate as such, so even if a terrorist attacked, we do not have to disrupt that. Thank you very much.

Senator COLLINS. I think it is interesting that at every single hearing we have had, no matter what the areas we are looking at, we find that agencies are not talking to one another or not sharing information or there is a lack of coordination. That is the common theme, whether we are talking about immigration policies or airports or our seaports. It does seem to be something that ought to be able to be solved.

Ms. DeBusk, I want to ask you about a comment you made about having voluntary standards for port security. You expressed some concern that voluntary standards might not be enough. What particular standards do you think need to be made mandatory rather than leaving it up to the individual ports?

Ms. DEBUSK. Firearms would be an excellent example. I do not know why you would want anyone with firearms to just be strolling around at the port, so I do not know why you could not just say, no, you cannot have firearms at the port, as opposed to see if ports want to have—you put out a guideline that says it is better if you do not have firearms at the port. That would, to me, be a perfect example.

Senator COLLINS. Mr. Quartel, I am very intrigued by the notion that both you and Mr. Flynn brought up of pushing the borders back. If we can inspect at the point of origin, it seems to me that really is the way we have to go, because if we do not inspect until the container gets to the United States, and we know we do not inspect most of them in any event, it is too late in many cases.

Assuming we could get agreements from countries and companies to have a system that pushes the borders back, do we have the technology that would allow us, once a container is inspected, to electronically seal it and alarm it and have a monitoring system? I am just unfamiliar with the technology in this area. Does that exist now?

Mr. QUARTEL. Some of that technology exists, and I think one of the later panels is going to be talking to the specific physical aspect of technology. If I might, I think what I would like to conceptualize for you, though, is a non-physical means of inspecting, which is really, I think, what we are suggesting to you here.

In the hierarchy of things you want to do, you want to first screen a cargo electronically. You know the data. You can funnel out 80 percent of it just by knowing with some certainity that they are good people, they are good companies, they have security in place, you know they maintain it. Then you go to a scan. There are passive scans. There is an issue there of the cost, which you will probably hear about later, and we cannot mandate that a foreign port use it. Then you go to search, and then you go to actually seizing it. So it is screen, scan, search, stop, basically.

There are technologies for the physical control of the process. They are a lot more expensive than most people can actually afford to introduce across a system of 40-some million containers worldwide.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins.

Senator Cleland, good morning.

OPENING STATEMENT OF SENATOR CLELAND

Senator CLELAND. Thank you very much, Mr. Chairman, and thank you for having the hearing today. Thank you, panelists, for coming.

I would just like to follow up on Senator Collins' observation. I am on the Commerce Committee as well as this Committee. Whether we are talking about aviation security, bus security, port security, rail security, homeland security, it does seem to us that, and to me as I connect the dots, that we are talking about three basic bugaboos: Coordination, cooperation, and communication between and with Federal agencies. Now, that is no rocket science there, but it is coordination, cooperation, and communication.

I have been briefed on the Dark Winter exercise, the attack or presumed attack by smallpox on the country, and Senator Nunn played the role of the President with the Johns Hopkins mock attack on smallpox back in June. That exercise was called Dark Winter, and Senator Nunn, who was in this body for 24 years, former chairman of the Armed Services Committee, said, as President, as he got into the mock exercise, he found himself becoming more and more impatient with bureaucracy. What he was running across was the lack of coordination, cooperation, and communication.

[The prepared statement of Senator Cleland follows:]

PREPARED STATEMENT OF SENATOR CLELAND

Mr. Chairman, as a Senator from a State with several ports, I appreciate your holding this hearing today.

I am also a member of the Senate Commerce Committee, which has oversight of our Nation's seaports. I welcome our chairman, Senator Hollings, here today to tell us what the Commerce Committee has done to help secure the Nation's ports. I supported these efforts, and voted for S. 1214, the Port and Maritime Security Act of 2001. Given the 2000 Report of the Interagency Commission on Crime and Security in U.S. Seaports which found that security at U.S. seaports "generally ranges from poor to fair, and, in a few cases, good," there was not time to waste after this country realized its vulnerabilities on September 11.

S. 1214 contains several provisions that I believe would help strengthen port security. The bill calls for a vulnerability assessment at our ports, and the review of this assessment should involve all relevant authorities for each port, which usually includes local, State, and Federal officials. At the Nation's 50 most economically and strategically important ports, the vulnerability assessment would be updated on a regular basis. The Department of Transportation would develop procedures for screening passengers, cargo and crew members at maritime facilities, and those employed at security sensitive jobs at ports would have to undergo criminal background checks. Attempts would also be made to work with foreign ports to assess security vulnerabilities abroad, which is an important part of this equation. Also, S. 1214 authorizes loan guarantees and grants to help fund security improvements and upgrades. This bill provides for funding of research initiatives to develop technology for detection of chemical and biological agents, which is vitally important as we continue to hear of the potential that terrorists may have access to "dirty" bomb materials. Unfortunately, there have been some Senate colleagues who have blocked consideration of this legislation despite the efforts of Senator Hollings and others to bring this bill to the floor. I am hopeful that we will be able to address this bill soon.

Since September 11 was not an attack on our ports, it is difficult to raise this issue with the public in order to have the public demand action. But, the facts point to the need for better port security: 95 percent of foreign goods enters or leaves by ship, only 1-2 percent of cargo containers are inspected, and the U.S. has 95,000 miles of shoreline. In Georgia, over 12 and a half tons of cargo on over 2,500 vessels entered our State ports during fiscal year 2001. I must be able to reassure my constituents and all Americans that the vast amount of material entering the U.S. via ship is safe. How do I do this under the current regime? I hope to get some answers today from our panelists.

Senator CLELAND. Now, how do we improve that? I just want to ask some basic questions based on the fact that I have a State which has two major ports, Brunswick, Georgia, and Savannah, Georgia. As a matter of fact, Brunswick is very close to the Trident nuclear submarine base at King's Bay, which stores nuclear weapons. That has been a real eye-opener to see how the lack of security at Brunswick, the Port of Brunswick, impacts, say, a nuclear sub base just to the South and how the nuclear sub base has had to take extraordinary measures just to protect its nuclear weapons.

I will say first, Mr. Commander, since the President says we are at war and the Coast Guard is supposed to be under the Navy, coordinated by the Navy in wartime, are we remiss by not having the Coast Guard under the Navy so at least at a nuclear submarine base like King's Bay, you have the coordination built in because the Navy is in command of the Coast Guard and the Coast Guard could help out with the protection of nuclear weapons? I just throw that out to you.

Mr. FLYNN. Sure, Senator. The cooperation between the Coast Guard and Navy has always been ongoing. Of course, even the Vietnam War, the Coast Guard was actively involved in the Vietnam War. We did a lot of river patrols and so forth, but we never felt officially under the Department of Navy in that instance.

Today, in fact, you have the CND offered to Admiral Loy naval assets to assist the Coast Guard in this new war, that is, helping in the patrolling, giving some Naval patrol craft to help the Coast Guard do its mission. You already have a Maritime Defense Zone Commander who is a Coast Guard Commander who is dual-hat and works with the Atlantic Fleet Commander.

So I am not worried about the ability for the Coast Guard to work with the Navy in an integrated way. I am more worried and concerned about the rest of that tapestry.

What we know about these terrorists is that they are blending into the real estate. They are blending into the day-to-day movements and trying to look as legitimate as possible, whether it is as a fisherman or a charter boat or whatever might be on the water, or that their commerce blends into legitimate commerce, and we are trying to get a handle on the people, the conveyances, and the cargo and have a sense of being able to fuse the details of that in advance.

The Coast Guard will have some knowledge about the conveyance, in this case a ship. That actually works. Our intelligence people sit with the Office of Naval Intelligence and the Navy works closely with that, as well, in tracking those.

Customs will know about the cargo and INS will know about the people, and obviously Consular Affairs, who give the visas, will know about the people. The FBI and CIA will have the backlist.

The challenge here, just to illustrate quickly, though, is—I heard this from a Customs agent who was involved with designing a scenario, he said, last April that followed this weapon of mass destruction, the container, and it was built out of—the FBI had given Customs some information about a household goods from Asia which actually had a dirty bomb in it and it was going to be arriving in New York on the Fourth of July. This had to go up to headquarters to get scrubbed before they used it. It got kicked back initially.

They said it was unrealistic because the FBI would never give the information about the household goods being contaminated to the Customs organization.

Senator CLELAND. May I just interrupt? Mr. Chairman, we have run across this with the CDC——

Chairman LIEBERMAN. That is right.

Senator CLELAND [continuing]. A couple of times—and we just had the Postmaster General here—we have demonstrated in hearings that the FBI, once it gets hold of the anthrax letters, whether it is Senator Daschle's letter or Senator Leahy, does not send it to the CDC. It sends it to Fort Detrick, Maryland, who does it, and Fort Detrick, Maryland, looks upon that as the FBI as a customer, so they are not going to tell anybody, and the FBI does not tell anybody. Therefore, the CDC winds up in the dark and ultimately gives bad advice to the Postmaster General about a Postal Service entity one step removed from Daschle's office while two people are dying at Brentwood.

The point is that it is not healthy for the right hand to not know what the left hand is doing. Again, coordination, cooperation, communication. So I just want to get your take on whether the Coast Guard, since the President said we are at war and the Coast Guard in wartime is under the Navy, ought to be under the Navy, but that is not your concern. Your concern is working with the other entities, right?

So let me move on to Ms. DeBusk. You mentioned the possibility of the fact that there is no central authority, controlling authority, in terms of port security in America. You mentioned the creation maybe of a Department of Homeland Security. As a matter of fact, that is exactly what the Hart-Rudman Commission recommended over a year ago, that an entity, an agency with budgetary authority and troops, people, infantry to command, be instilled in our Federal Government to coordinate this kind of thing.

Instead, we have an Office of Homeland Security with 18 people. Tom Ridge is a good guy, a fellow Vietnam veteran, but I doubt that 18 people are going to go up against 60 different agencies. So we still are left with the challenge of coordination, cooperation, and communication.

Any thoughts about what this Committee ought to do in furthering our strong interest in strengthening an Office of Homeland Security or creating a Department of Homeland Security?

Ms. DEBUSK. Yes, and I think you have already answered the question and that is resources. The only way you really get good coordination is through resources to back it up in addition to jawboning and saying, let us all talk together.

The resources would come in for basic things like computer systems that talk to each other. There is a lot of good will in the agencies. They like to cooperate. For instance, my former office got along excellently with the Customs Service, but we did not have the same database for going back and forth on the computer system with the information.

And so I think in terms of getting coordination and the concept of pushing back the border, it only works if there are resources that would be committed to doing things like letting the agencies talk to each other over the computer system.

Senator CLELAND. Thank you very much. My time is up.

Just to highlight, I mentioned this in the Commerce Committee, I will mention it here, that Georgia Tech in Atlanta has developed a little chip, a little glass sensor to pick up biological and chemical agents, which might be helpful in this war against terrorism and detecting early on what is in some of these containers.

Thank you very much, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Cleland. That is very interesting. You know, you are right. Something is going on here, and probably my colleagues on the Committee have had the same experience I have, which is that a lot of complaints from local officials about difficulty in working with the Federal intelligence agencies and the FBI. I wonder if the Committee might not have a role to play in calling in the agencies, either in a public or private session, and talk about this problem. The examples that you just gave, Dr. Flynn, and I think it was Rear Admiral Larrabee gave another example earlier on, they are just not acceptable, because you are now—ports are now the front lines, so we have got to arm you with the information to protect us.

Senator Bennett.

OPENING STATEMENT OF SENATOR BENNETT

Senator BENNETT. Thank you very much, Mr. Chairman, and for your pursuing this continued issue. In the spirit of full disclosure, I am going to be very shameless in pushing my bill.

Chairman LIEBERMAN. It would not be the first time that has happened around Congress. [Laughter.]

I was not speaking of you, but it has been done in Congress before.

Senator BENNETT. Right. In July, the Defense Threat Reduction Agency, DTRA, gave me a top secret briefing on air vulnerability analysis of the Port of Baltimore, and, of course, the members of the panel might not know, but my hobby horse, my focus here is on critical infrastructure protection generally, but the computer portion of it more specifically.

Some people say to me, well, why are you focused on computers because homeland defense, homeland security involves so much more than computers. I will give you an example that I use in speeches. With the ability that currently exists for hackers and others who want to get into computers, this is not a theoretical. This has happened. Someone got into the computer system at a dam and was in a position to control whether or not the floodgates would be opened or closed. Downstream from the dam was a military installation which would have been flooded and destroyed had the hacker or activist or whoever it was decided to open the floodgates.

So when you think of homeland security and you want to protect the military installation, or fill in the blank, put in whatever you want, downstream, you want to protect the facility downstream, it was the vulnerability of the computer that made that possible.

And as I sit here and listen to all of you describe your frustrations and your problems, I realize that we cannot stovepipe port security away from the issue of computer security. You talk about anomalies, Commander Flynn and Mr. Quartel, you wanted to look for an anomaly in the situation, suppose I was the individual load-

ing that dirty bomb in a place where it would not show up, should not show up, and that would be an anomaly that would immediately appear on a computer screen somewhere. And prior to learning that, I break into the computer system and change the data so that the data that comes says this is not an anomaly. This really is woolen goods or cotton goods or something coming from an agricultural country, and yes, it has an unstable political background, but these are T-shirts that we do not need to worry about because I have changed the computers to have the information that comes to you say it is T-shirts.

And when we talk about the theme that Senator Cleland talked about and Senator Collins talked about of not talking to each other and not getting the proper analysis, we come back to the fact that I have heard several of you say a very large portion of the ports are under private control, and unless we pass a law that requires private people to give us all of the information as to what is happening in terms of the threat on their computers, which law does not exist now, again, shamelessly, we need to pass my bill which says they can voluntarily share that information with a common analysis center in the government without worrying about a FOIA request being filed by Osama bin Laden saying, I want to know what the private sector is telling the government about my attempt to break into their computers.

So, as I say, shamelessly, I am laying this out. Now, I would like your responses to that and your comments about that and see if I have misread some of your testimony about vulnerabilities here.

Mr. QUARTEL. I actually have not read your bill, but I like what you are saying. In the specific example—by the way, I have also a port story. I was at the Port of Los Angeles Tuesday afternoon and they had a similar story to this one about information sharing. There are reasons for not information sharing, which we know, firewalling various kinds of data. But there are also ways to share data by tapping databases electronically without violating all of these other provisions, which I think is what you are talking about.

No terrorist is going to tell you he has got 20 tons of nitrate kinds of fertilizers and a $80 GPS and a $3 blasting cap that he is going to load through there. There is a hierarchy of responses. Data by itself will not tell you anything.

Customs today has a program they call BASC, for example, which they use in the drug process, where they work with trusted parties, people who have procedures in place where they seal and load and they know the people there, they have security as to who the people are, so they can actually certificate across the process and that helps them speed it.

So while you use data to look for anomalies and suspect situations, you also do what Steve Flynn was saying, which is you also can channel big chunks of that out. If it is a Cisco, for example, they may have a procedure in place that you cannot load a nuclear weapon or a dirty bomb in any of their systems. So maybe those cargoes go through faster.

There may be small players in the business who can also get through that process. In fact, most of our cargoes that come from Asia have a lot of small players, so we actually have to deal with the real world as it really is.

If I have one message to the Committee beyond that I have already said, it is that what we should do is tap into the way business works, and one of the things as government we do not do very well, particularly in transportation, is ever ask the shipper, meaning the guy who owns the cargo, what they think. We go to the carriers, we go to the labor unions, we go to this, we go to that, but we do not go to the shipper, and these are the guys who have the holistic view of the process.

We have talked about tracking. Most shippers do not care where a cargo is every minute. It is not useful data. What is useful is to know it arrived at the port or it is going to be 3 days late at the port or it missed the train, because then they use it for planning.

So if we talk about tracking, for example, it should align with what a customer wants to do with it. It should align with his commercial interests. And if we do not align the interests, you are going to find things like port shopping.

Senator Hollings said, well, let us concentrate on the top 25 ports. You should, but on September 11, the guys came through a minor airport, an out-of-the-way crossing at the border, and then fed into a major funnel and you will have exactly the same kind of thing in shipping unless you align your interests with the way the commercial sector operates and data is a key part of it.

Ms. DEBUSK. Let me just add something on that from one of the concerns of the private sector, because the security of the data is incredibly important for getting the cooperation of the private sector.

Senator BENNETT. That is right.

Ms. DEBUSK. One of the big concerns is the very mundane concern of theft. If you know exactly what is coming in, exactly where it is, you can find it exactly with this high-tech device. It turns out that it is great new color TVs, which, unfortunately, can disappear before reaching its final destination. So a major private sector concern in trying to do the public-private sector cooperation on data would have to be addressed through the security of the data.

Senator BENNETT. That is exactly the point of my bill. It says you can share this information and it will stay secure within the government.

Ms. DEBUSK. And also secure within the government, and then you have to think about a limited number of people within the government that would have access encrypted passwords, the whole thing.

Senator BENNETT. Sure.

Mr. FLYNN. And absolutely, Senator, I would support this, as well. You find most sophisticated ports are actually run virtually by computer, the gantry cranes and everything else. You take down the computer system, you shut down that port, as well. So the cyber attack could do it as much as a physical bomb kind of thing with huge disruption effects, so there is that area.

The other is, ultimately, of course, we must be talking about sharing data overseas. We are dealing with multinationals, not just private sector domestic, but multinationals, and we are also, as with Canada, in an effort to enhance our data shopping there, if there is not comfort about the security of the data, that is going to make that much more problematic.

I think taking that wartime analogy, though, that we are in, as the President said, about trying to apply it in this area, I think it would behoove us to think about—I get from a number of private sector people up in New York who have really been, obviously, mobilized by the tragic events of September 11 and are waiting for the call, basically. These are the people who understand how to do data management, understand how to do data mining. We have huge companies out there who solved how to bring legacy systems together and make mainframes go and they are just sitting idle.

I think some calling in of a red team, almost, to solve this information issue from private sector folks, anoint them, give them 9 months' charter, give them all the resources they need to fix this problem. Everything we are talking about in the government is 5- or 7-year, multi-year programs in one sector that we are not going to finance anyways until whenever. That is unacceptable. I do not think we are going to fix it through our traditional public sector needs. If it is a wartime, let us treat it as such and fix this by getting the smart people into this.

Senator BENNETT. That is a good summary, because in World War II, a lot of information from the private sector was considered secret, classified, shared with the government with the understanding that it would not be available, and in the war we are talking about here, with 90 percent of the critical infrastructure in private hands, that means an intelligence officer trying to see what is happening on the battlefield has 90 percent of the battlefield blacked out to him if the private sector does not share the data. But as you indicate, Ms. DeBusk, the private sector will not share the data if they think it is going to be made public.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Bennett. Your questioning may have been shameless, but it was quite productive, I thought, and very interesting.

Senator Thompson.

OPENING STATEMENT OF SENATOR THOMPSON

Senator THOMPSON. Thank you, Mr. Chairman. Sorry for being late. I was a witness this morning, an uncustomary role though it may be, at a U.S.-China Commission hearing. I wanted to get over here as quickly as I could.

Chairman LIEBERMAN. We are glad you are here.

Senator THOMPSON. It occurs to me in listening to this that one of the things that is happening here is going to cause us to really look at the issue of federalism in a different way. One of the things this Committee deals with, of course, the relationship between the various levels of government.

I listened to you and once again we see various Federal agencies are involved to one extent or another, but so is State, so is local. And, law enforcement is on one side, while prevention is on the other. The real question, I think, that we are grappling with is who ought to be doing what? What should we be doing and who should be doing it? If you think about it, that is really the main question of the government and it is not an easy one.

I think that what we are seeing now after September 11 is that we are going to be doing some reassessing and we are probably

going to be bringing the Federal Government into some areas, at least on the prevention side, that maybe they have not been before. We need your help on that.

Hopefully, we will learn to stop doing some things at the Federal level that we should not be doing and let those responsibilities go to the State and local governments. We should consider a realignment, a reprioritization, as it were, to look at federalism anew and start concentrating and spending more of our resources on the things that the Federal Government can do and must do best. We should look for standardization. I think in areas of national security, we have to really look at that.

The other thing that is kind of related that concerns me is what is the economic impact of all of this going to be and what are we going to be willing to tolerate. We can devise all these systems, but as we have seen at the bridge in Detroit, a little bit of slowdown, a little bit of disruption and things start backing up. What is that going to do, what is our toleration level going to be, and to what extent are we going to have to start looking at things differently?

We have been called upon to sacrifice in this country, but so far, about the only sacrifice we have been called upon to do is shop at the mall, and buy more. What if we have to get used to doing more, not just at our airports, but here?

My testimony today before the China Commission had to do with the extent to which we should be allowing foreign companies that are engaged in proliferation activities, that our government determines that are engaged in proliferation activities, to raise billions of dollars in our capital markets, no questions asked, without disclosing to the investors that they are engaged in proliferation activities.

It seems like a no-brainer to me, but that is what is happening, billions and billions of dollars by companies, including Chinese companies that our country knows are engaged in proliferation activities, making the world more dangerous, which we say we need a national missile defense system to protect us against. But they can come and raise billions of dollars and hand it over to the military, as far as we know.

As I am speaking, half of Wall Street is downstairs explaining why I am wrong because the measures I recommended will not do any good, because they will have an economic impact, it is going to cost us business. How much are we going to be willing to do? Has anybody made an assessment of the economic impact of the preventive measures that are being put on the table?

Rear Admiral LARRABEE. In the Port of New York and New Jersey, we have estimated that it will cost us about $150 million in the next couple of years to implement just some of the things that the Hollings bill has suggested. As we begin to talk about other ways to prevent terrorism, I think that the cost goes up.

You are absolutely right. My job every day is to find a way to balance a system that works very well because of its speed and its economy with the need to slow it down and be more deliberate in terms of making sure that we know what comes across the border, and that is a very, very difficult challenge, because the system that we operate today is what drives the engine of our economy, and the minute that that system slows down and we cannot bring oil in on

the basis that we bring it in now, the system comes to a grinding halt.

Mr. QUARTEL. If I can add to that, too——

Senator THOMPSON. Liquid nitro gas, which is very much a concern.

Mr. QUARTEL. Maybe I can take it from the micro to the macro. Every trip I now take on an airplane, and I used to travel a lot, adds 4 hours. That is half a day. So I travel 80 percent less. So I am certainly not helping the aviation system, nor, frankly, are a lot of the rules, the way they are being implemented across the system.

In logistics, the cost of transporting and moving goods and logistics and storing and maintaining them as inventories in the United States 20 years ago was 25 percent of GDP. Today, it is 15 percent. We have saved $1 trillion annually in terms of the kinds of things we have built into the system by moving cargo swiftly, reducing inventories, reducing the cost——

Senator THOMPSON. Just in time?

Mr. QUARTEL. Just in time. Although even "just in time" is only in a small percentage of the economy, these things affect everybody, from the biggest to the smallest.

Senator THOMPSON. Some people are saying we are going from "just in time" to "just in case" now.

Mr. QUARTEL. Well, there is some issue there, but let me give you a number there. If you only increase inventories by 5 percent, you add $75 billion in costs to the American economy. That is 75,000 jobs you have just lost.

Mr. FLYNN. I might add here, though, I think the key, again, about this prescription, if we are willing to take this in a comprehensive networked approach, Rear Admiral Naccara, the First District Commander up in Boston, has a very creative and ultimately successful model for how to deal with the liquified natural gas. What he is doing is he is sending inspectors to Trinidad where it is loaded. They are inspecting the facility, which actually is a pretty good, secure facility, to board the vessel when it leaves the harbor, inspect it before it goes to make sure there are no bad people on it, sail the harbor and get off at the pilot buoy. If it was hijacked in between, there would obviously be some communication of that.

The advantage is when it gets to Boston, we are actually able to speed it in. I mean, you are going to still do some controls, but you do not want it harboring out there for a few days having a big advertisement, LNG is waiting here as a target. You actually want to get it in relatively quickly. So they will be met with an escort, but it will be moving very quickly. The company loves it because it now has expedited treatment in. We are more secure.

The same modeling applies, I think, even as we think about cargo. If we are talking about building this in as a standard up front, the market will adapt, I think, to it.

I would propose that, for instance, that perhaps Governor Ridge—well, the President would issue a homeland security Presidential directive to the Secretary of Transportation to meet with his counterparts in the six or seven major megaports to essentially say, we are not going to allow mystery boxes anymore into our

ports because they are a critical infrastructure and here are the standards. And as soon as that is harmonized, the cost issue starts to get adjusted, just as it has with oil tankers.

When we had this real problem many years ago, there were a lot of unsafe tankers, people were saying we could not impose standards. The oil would not come in anymore. Well, we have rationalized and adjusted.

The real cost, though, for me, the one that most keeps me awake almost every night, knowing what I know about the system, is the cost of turning the spigot off. Ninety-five percent of general cargo coming into the United States comes in a container. This makes the anthrax in the mail service pale by comparison. We went to E-mail and faxes and UPS and FedEx. When you compromise this system and you turn off the switch, there is no alternative. Cargo stops coming in. That is the cost matrix I think we need to balance against, the dollars that we are talking about here and putting in a smart approach.

Senator THOMPSON. Ms. DeBusk.

Ms. DEBUSK. Yes. One of the important things that is in the Hollings legislation, and that was recommended by the Seaports Commission, has to do with threat assessment. Because it is simply not possible to do everything that we can or should do at every single one of the 361 ports. So an important way to weed out spending priorities would be to conduct threat assessments and figure out where the greatest vulnerabilities are and tackle those first.

Rear Admiral LARRABEE. And then with better information, you can adjust your reaction with the idea that you cannot do everything, and——

Senator THOMPSON. It seems to me like a threat assessment, certainly, everything has got to be prioritized and all that, but it looks to me like once we do that, it has got to be the most closely held information in all of our government.

Ms. DEBUSK. I agree.

Senator THOMPSON. If the bad guys have that information, then it is all for naught.

Ms. DEBUSK. I agree completely, and even some of the information that was put out by the Seaports Commission is no longer available.

Mr. FLYNN. On the reverse, I just might say, Senator, is the schemes that we talked about, the criminals are there. They know—we are not talking about a hypothetical—about containers being used. They have been used for the last 15 years to smuggle narcotics into this country, as a matter of routine, almost. So bad guys know the vulnerabilities of this system.

Mr. QUARTEL. And I would suggest to that, every one of us can tell you how to get it in, and if we can, someone else can, as well.

Senator THOMPSON. Knowing what we are watching and what we are not watching is what I am talking about.

Mr. FLYNN. Oh, yes, sir.

Senator THOMPSON. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Thompson.

Thanks to the four of you. We have got to move on to the next panel, and we really did not go into some of the very big ideas that you gave us for reform, such as pushing the border back and how

that would work, how we station our personnel there or do we, and does that require international treaties and agreements. And then, although we will get into both of these matters in the next panel, too, I hope, the use of technologies that are available now to create new ways to track containers without slowing them up so that there is no adverse economic effect.

Perhaps either with the Committee or our staffs, we could ask you to give us some more time to better develop those ideas, because it may be that this Committee can take a leadership role, hopefully after Senator Hollings' bill is passed, which I hope will happen soon, to implement some of those ideas.

But in the meantime, I thank you very much. It has been excellent testimony.

Chairman LIEBERMAN. We will call our third panel, Argent Acosta, Customs Inspector, Port of New Orleans, and President of the NTEU Chapter 168; Deputy Chief Charles Cook of the Memphis Police Department; W. Gordon Fink, President of Emerging Technology Markets; and Michael Laden, President of Target Customs Brokers, Inc.

Thank you all for being here. Chief Cook, we are going to call on you first. You come from a great city.

Mr. COOK. Thank you, sir.

Chairman LIEBERMAN. You even have some great Senators representing your State here in Washington.

TESTIMONY OF DEPUTY CHIEF CHARLES C. COOK,[1] MEMPHIS POLICE DEPARTMENT

Mr. COOK. Thank you very much, Mr. Lieberman. I would like to say good morning to the Members of the U.S. Senate, witnesses, and others present. I want to give special thanks to Senator Fred Thompson and, in particular, his staff, Hannah Sistare, Jason Roehl, and Morgan Munchik, for inviting me to speak here today on behalf of the people of Memphis.

I am here today to talk about the City of Memphis, how we have responded to the events of September 11, and the needs of Memphis in the area of homeland security. I am sure our situation is much like those of other cities our size.

Prior to September 11, the Memphis Police Department, the local FBI, the Memphis and Shelby County Emergency Management Agency, the Memphis and Shelby County Fire Departments, the City of Bartlett, the City of Germantown Police and Fire Departments began training with incident command tabletop exercises. Our focus was on natural disasters, the threat of terrorist attacks, school shootings, and plane crashes.

This multi-agency training developed a team concept in responding to large-scale, long-duration events. Our departments began seeking further training for various contingencies. In all the exercises, role players simulated their responses, and as a result of the critiques and follow-ups, they determined that additional training, equipment, and manpower resources were needed.

Because of extreme delays on the Memphis to Arkansas bridges across the Mississippi River at I–55 and I–40 caused by relatively

[1] The prepared statement of Mr. Cook appears in the Appendix on page 120.

simple accidents, a multi-agency bridge mitigation team was formed in the year 2000. Members of this group came from the police departments of Memphis and West Memphis, Arkansas; the sheriff departments from Shelby County, Tennessee, and Crittenden County, Arkansas; the Tennessee Highway Patrol and the Arkansas State Police; the Railroad Police; the Tennessee and Mississippi Departments of Transportation. Various casualties, including marine accidents, terrorist attacks, and any subject threatening bridge security became topics of discussion. Decisions regarding multi-agency jurisdiction and removing hazards from the roadway were made and the agencies took joint responsibility for patrolling the bridges and they continue to do so.

Most police, fire, and emergency management agencies during the first few hours of September 11 reacted by encircling the government buildings in the downtown area. We deployed our resources to include other targets of opportunity, including bridges, water supplies, power utilities, and similar government-related services. We received numerous phone calls from businesses, manufacturers and trucking firms, refineries and other facilities. Each caller was interested in information on what to expect in the way of local terrorist attacks.

Their questions were addressed through the media in a press conference with public officials, including the Memphis Mayor, the Shelby County Mayor, the Police Director, the Shelby County Sheriff's Chief Deputy, the Fire Director, and other emergency services personnel. These officials made an evaluation of the immediate threat to the city based on information from the FBI and national and local television news. This resulted in an agreement that our response could be reduced at that time. Jointly, in an organized setting, this team of city officials released information to the public. It was timely, informative, and reassuring.

We have continued to maintain high levels of alertness, giving special attention to large sporting events, concerts, and the Beale Street entertainment district. We have experienced a blow to our budget as a result of September 11 and our anthrax responses. Sustained actions resulting from hoaxes, threats, and actual attacks are devastating to local budgets, as you know, draining dollars by eating overtime. There is little that can be held in the hand following unbudgeted responses.

Since the events and continuous warning of future threats, many cities are looking at budget shortfalls. We have still maintained high levels of awareness and are establishing communications between our precincts, manufacturers, and redistribution.

Following the New York attack, we have experienced the uncertainty and fear of bio-terror. There have been several warnings of additional attacks. As we further assess our ability to deal with attacks of this type, it is necessary to evaluate what is needed in order to defend ourselves against attack, to respond to and reduce the damage and loss of life, and to fully recover.

In reviewing the needs of the city, I must mention the Port of Memphis, an integral part of the Memphis economy. Memphis is known as America's distribution center. I think this notoriety comes from its association with Federal Express, the United Parcel Service, and other air carriers. However, the marine port facilities

of the Memphis metropolitan area is one of only three cities served by five class one railroad carriers serving 48 contiguous States, two barge fleeting services, and a multitude of barge and truck transport services. International shipments come through the Port of New Orleans and are filtered to the other States through Memphis, the world's largest cargo airport hub.

The Port of Memphis is the fourth busiest inland port in the country. The port facility has immediate access to Interstate 40 and Interstate 55 and is located less than 15 minutes from the Memphis International Airport. The Port of Memphis also provides a unique industrial area for the convergence of transportation services located near the Memphis downtown district.

This transportation hub has been of interest to organized crime due to the large quantity of manufactured goods. The Memphis Police, the Shelby County Sheriff's Office, the local FBI, the U.S. Customs Service, and the National Insurance Crime Bureau was organized through a memorandum of understanding, updated yearly, into the Tennessee, Arkansas, Mississippi Auto Cargo Theft Task Force. This is a multi-agency investigative law enforcement unit targeting organized vehicle theft, including heavy equipment and farm and construction machinery, and associated criminal activity and thefts from interstate cargo shipments. They are involved in activities in and around both marine ports and the airport.

These are the reasons Memphis is considered to be a potential terrorist threat.

The following are suggested measures which should be considered in the interest of preventing terrorist attacks, attacks which would severely interrupt interstate commerce for years if successful, seriously crippling the Nation.

Use a multi-agency approach to the investigation of suspected terrorists and develop the availability of an electronic clearing house for all information gathered nationally and internationally on suspected terrorists.

Assign fully-armed U.S. Coast Guard personnel to 24-hour operations, providing visible patrols on the Mississippi River, Wolf River, McKellar Lake, Tennessee Chute, and the new Frank Pidgeon Industrial Park.

Support a national or international truck driver licensing program for drivers entering and exiting the U.S. from Canada and Mexico and for crossing major infrastructures, bridges, and tunnels. Also, support technology capable of identifying drivers and driver history by fingerprint, photos, and newer iris scan technology for officers to use in the field.

Support smart card technology for trucks and loads, capable of immediately identifying driver, cargo, origination point, destinations, and route plans. This would also do well for marine vessels.

Organize a U.S. Coast Guard inspection boarding team to meet and board vessels above and below the Mississippi River bridges to identify operators and crew and to monitor approaches to sensitive infrastructure, such as bridges, industrial complexes, and production facilities with river access.

Assign U.S. Army or Army Reserve troops to provide 24-hour security and surveillance to the more critical targets, where attacks would cause severe repercussions for America.

Provide security gates and barricades limiting access to Presidents Island, refineries, and chemical plants from vehicles without proper identification and authorization.

Establish privately-owned police agencies, like the Railroad Police and Federal Express Security Police, for the protection of businesses which produce or manage critical materials.

Also, establish a Homeland Security Block Grant to meet such needs as police and fire overtime, training, communication and rescue equipment, and for security measures to protect airports, waterways, utilities, public transit, and other public infrastructures.

Thank you once again for inviting me here to testify today. I will be happy to work with the Committee in the future in any way and I will be glad to answer any questions you may have.

Chairman LIEBERMAN. Thanks, Chief Cook. That was excellent testimony and I appreciate the specificity of the recommendations. We are going to hold a hearing in the Committee, I believe at the end of next week, particularly having local officials come in from around the country to talk about some ideas, and the idea of federalism Senator Thompson talked about earlier. But your proposals here really set the table for that and I appreciate it.

Mr. COOK. Thank you, sir.

Chairman LIEBERMAN. Mr. Acosta, thanks for being here. You bring firsthand experience as a longtime Customs inspector and we appreciate your willingness to be here and look forward to your testimony.

TESTIMONY OF ARGENT ACOSTA,[1] SENIOR CUSTOMS INSPECTOR, PORT OF NEW ORLEANS AND PRESIDENT, NATIONAL TREASURY EMPLOYEES UNION (NTEU) CHAPTER 168

Mr. ACOSTA. Thank you. Chairman Lieberman, Members of the Committee, thank you for inviting me here today to talk about port security. My name is Argent Acosta and I am a Senior Customs Inspector at the Port of New Orleans. I am also the President of Chapter 168 of the National Treasury Employees Union. My chapter actually encompasses five States, Louisiana, Mississippi, Tennessee, Arkansas, and Alabama. There are 19 ports in that region of Customs and the majority of those are seaports.

I have been a Customs inspector for 30 years, the Chapter President for 26 years. My job is to ensure that illegal contraband, from knock-off designer jeans to cocaine to bombs, does not enter the country, and that legal goods that enter the country are assessed the correct duties.

At seaports like the Port of New Orleans, the mainstay of the job is boarding incoming vessels, primarily cargo ships, to inspect for illegal goods. It can be a very dangerous and not very glamorous job, but there is a great deal of commitment by the front-line inspectors to do the best job possible, especially since the events of September 11.

I would like to share with the Committee a recent example of that commitment. Inspector Thomas Murray, a 31-year veteran of the Customs Service, died tragically during an inspection of the hold of a vessel at the Port of Gramercy, Louisiana, on October 30

[1] The prepared statement of Mr. Acosta appears in the Appendix on page 127.

of this year. He was killed by toxic fumes, as was a member of the vessel's crew and the ship's captain, who followed him into the hold. A second Customs inspector was overcome by the fumes, but is recovering.

Inspector Murray was aware that the vessel he was searching previously brought illegal drugs into the United States, so he was determined to be as thorough as possible. He did not know what dangers he would encounter when he went below the deck, but he went anyway. Tragically, his commitment to doing his job, despite potential danger, cost him his life. His fellow inspectors, especially those of us from Louisiana, will mourn his loss for a long time to come, but we will also remember his bravery and commitment every time we are faced with boarding a suspect vessel or searching a hold that we believe to be dangerous.

Mr. Chairman, you asked in your letter of invitation that I address several questions regarding port security in my testimony. The first was, what is the current adequacy of port security? I am afraid that I must answer that question by saying I believe port security is currently not adequate and poses serious potential threats to those not only in the immediate area of the port, but to those who may come in contact with uninspected material that arrives through our ports and moves throughout the country in other modes of transportation.

The Customs Service is currently only capable of inspecting about 2 percent of the 600,000 cargo containers that enter our seaports every day. From my own experience in New Orleans, despite the huge increases in trade since I started with Customs in 1970, the number of Customs inspectors at the Port of New Orleans has dropped from approximately 103 in 1970 to 29 this year. In addition, since September 11, Customs inspectors from around the country have been temporarily reassigned, primarily to Northern Border ports to cover the gaping holes in security there.

Since I had previously volunteered for emergency response team duty, not realizing, of course, that September 11 was on the horizon, I was among the first to do a temporary tour of duty in Michigan, at Port Huron, one of the busiest truck crossings in the country. On September 14, I was given 4 hours to go home, pack, board a Customs flight at the Gulf Port Airport and go to Michigan, at which time I found out I would be in Port Huron.

There was an incredible amount of pressure on inspectors at Port Huron since many "just in time" auto parts headed from Canada to the big three auto makers go through the port. I know my biggest personal concern was not to be the one who let a terrorist into the country, and some supervisors seemed to support that view, the view that extreme caution was necessary. However, others seemed to be sending the signal that we needed to move things through more quickly because of the need for the auto parts, so it is a very difficult balance and I can appreciate the problem that they are faced with.

I will begin another temporary assignment at Port Huron in January. These temporary assignments, while currently necessary due to the extreme shortage of personnel, leave home ports, like my Port of New Orleans, able to inspect even fewer vessels than usual. Also, the more an inspector knows about a particular characteristic

of his port, what the main goods that go through the port are, what are the main carriers, the destinations, etc., the more effective he or she can be. Obviously, 30-day temporary assignments at different ports does not lend itself to building this kind of experience.

The use of the National Guard at some ports may be temporarily necessary due to the unprecedented threats we are facing, but in many cases, due to their lack of training and experience in the area of cargo and vessel inspection, the National Guard provides the appearance of security rather than any real increase in security. In any case, having military personnel perform these duties is obviously not a long-term solution.

In addition to the severe limitations on the ability to do actual inspections, the technology that is supposed to help us do our jobs by providing us with advance information on oncoming vessels is outmoded, subject to brownouts, and often incompatible with the technology of those we need to communicate with. In addition, the advance information about what cargo may be aboard a vessel often is not sent early enough to do any good, and even more often is not accurate. Customs has determined through its own system that the accuracy rate of vessel cargo information is only 56 percent accurate, and let me give you a real current story to point out this aspect.

In April of this year, a vessel arrived from the Port of Savannah. It was a foreign flag vessel with containers on board for discharge throughout the United States. Our enforcement team targeted the vessel for boarding. We targeted the vessel to look at the cargo that was available. It had empty containers and full containers. By doing that, we set certain containers aside that we wanted to pull off and take a look at and we wanted to verify all the rest of the containers, including the fact that the empty containers were empty, and you will see why we do this.

We looked at the vessel and encountered one of the empty containers and upon opening it found out that it had cargo in it. We sealed the container and sent it to our cargo examination station. It sat for a day or two. When the two inspectors who worked the station went to open it up, their radiation detectors went off. They went off big time. One of the inspectors was our actual HAZMAT coordinator and trainer, so she backed everybody off, moved everybody away. We called in the experts. The container was very hot. It had drill testing, well testing equipment on it, but it was a serious threat to everybody around it. Fortunately, after testing and after a period of time, it appears as though the inspectors did not suffer any long-lasting effects. We hope they did not.

But were it not for us targeting the vessel and looking at the containers, this empty container would have moved throughout the country to wherever it was going to go, and whoever else who might have walked up to it who did not have equipment to note that there was something wrong with it might easily have been harmed or killed.

There are also problems with regard to the physical security of the port. Access to cargo and cruise vessels in many ports is not limited to those with prior approval to be in the area. Virtually anyone can gain access to the areas where vessels unload passengers and cargo. While there are secure areas in the Port of New

Orleans, access to those areas is overseen by contract security personnel, who, like airport baggage screeners, receive low wages and little training.

In fact, in the immediate aftermath of September 11, while Customs was and still is on its highest state of alert, I noted as I passed a secure area, the checkpoint going into the port area of the port, that there was no one in the security checkpoint. I sat for a few minutes thinking that maybe somebody had stepped into the bathroom, and it was the case. They had stepped away from the access. So access to the secure area was totally insecure.

The second question you asked me to address is what problems confront the Customs Service and other Federal agencies charged with securing our ports. I believe that the biggest problem is a lack of personnel. As I mentioned earlier, trade has grown exponentially. The number of airports, seaports, and border crossings have increased and have seen huge increases in passenger traffic. Funding and personnel levels have not kept up. I believe that funding is also an issue with regard to the use of low-wage contract personnel to provide security services to the port.

Another problem facing Customs in securing our ports is that I believe the balance between rigorous enforcement and facilitation of the trade can tip too much towards trade facilitation. In the aftermath of the September 11 attacks, there has been a renewed focus on our enforcement role and it has revealed great vulnerabilities. Yet we need to move trade and people throughout ports quickly, but we also need to make sure that we are doing it in a way that protects our security. In order to do both, we need more personnel.

Other problems mentioned earlier include lack of adequate technology and timely and accurate manifest information. It also includes the sharing of information.

The final issue you asked me to address was whether I had any recommendations to address the problems discussed above. The most important recommendation I would make is that Customs needs to be provided with adequate funding. In February 2000, the Customs Service commissioned a study, referred to as the Resource Allocation Model, that set optimum staffing levels for Customs at ports throughout the country. That report, which I would like to submit for the record, showed a need for 14,000 additional Customs positions. That was before September 11. I would hope that Congress would act to provide those additional positions.

I believe that there is also a need to look at recruitment and retention issues for Customs inspectors. The compensation and benefits are less generous than many State and local law enforcement officers and there is a serious concern that experienced Customs inspectors will leave to go to other professions, including the air marshals, due to the more generous compensation package, particularly in the area of retirement. Customs inspectors should receive the 20-year retirement benefit available to other Federal law enforcement officers if Customs is to remain competitive.

Customs also needs upgraded technology. Congress has provided initial funding for the Automated Commercial Environment, or ACE, system, which will make remote inspection of cargo more ac-

curate. I must point out, however, that this kind of technology can never take the place of physical inspection.

There is also a need to address the physical security issues at our ports by setting up secure areas for incoming cargo and personnel and by ensuring that port security personnel are well trained.

I would add just one more thing. Customs recently has entered into a program which has taken away the option of boarding vessels midstream for Customs. This really has serious consequences, because, in effect, it leaves Customs inspectors such as myself and my counterparts blind as to what is in a vessel sitting in the river.

Many vessels arrive in the Port of New Orleans. They go to anchor. They actually load or discharge their cargo all while at anchor, so we will never have an opportunity to board the vessel to fully look at the manifest, and we use—in the case of the radioactive container, there are many needs that we have to look at. We have to match all of these up just to try to come up with a picture that is reasonably accurate, and this is about accuracy.

I have heard other panel members discuss the fact that Customs' area of expertise is the cargo. I believe that is true. I believe it is supposed to be. But I want to impress upon you that, by our own study, 56 percent accurate is not a very good rate.

So we have to use whatever means that are available to us. That includes the vessel, the chief officer of the vessel, the information that the steamship line provides us, stevedore information. We get it from anyplace that we can, and then what we have to do is basically put all that information together and extrapolate what we think is the best possible picture of what is on the vessel.

Thank you. I would be happy to answer any questions.

Chairman LIEBERMAN. Thanks very much to you, Mr. Acosta. We have got a lot of work to do.

Mr. ACOSTA. Yes, sir.

Chairman LIEBERMAN. Mr. Laden, you bring a unique perspective and a very important one here as President of Target Customs Brokers, and that is the private sector, the customers. Thank you for being here.

TESTIMONY OF MICHAEL D. LADEN,[1] PRESIDENT, TARGET CUSTOMS BROKERS, INC.

Mr. LADEN. Thank you, Mr. Chairman. Mr. Chairman, Members of the Committee, good morning. My name is Michael Laden and I am the President of Target Customs Brokers, Inc., a wholly owned subsidiary of Target Corporation. I am also the current Chairman of the American Association of Exporters and Importers, and I am an appointee to the Treasury Advisory Committee on the Commercial Operations of the U.S. Customs Service, otherwise known as COAC. I would like to thank you for allowing me the opportunity to express my views under consideration today.

Without trying to become too prophetic or philosophical in my comments, the atrocities committed against us all on September 11 have forever distorted the way in which we as a people will live. It is reshaping and transforming the way we think about every-

[1] The prepared statement of Mr. Laden appears in the Appendix on page 133.

thing, security first, everything else second. "Just in time" for some companies has morphed into "just in case," adjusting lead times and building safety stocks to offset potential security delays.

Our industry, perhaps more than any other in America, will be deeply impacted just by the very nature of the business itself. As you have heard, the fabric of our industry is an intricate weave of very complex components and stakeholders. A single import shipment and the documents accompanying it pass through many hands and many different checkpoints as it travels to our country. Every one of those handoffs creates new vulnerabilities.

Now, before I continue with my comments, please allow me to make one very important distinction. I am not holding myself out as a security expert. I do rely on others, including the U.S. Customs Service, for advice and assistance. What I can offer this Committee today, however, is more than 25 years of practical operations experience in international logistics and on Customs matters.

Target's bottom line is this: We want no more nor any less than exactly what we have ordered when it comes to an international consignment. Simply put, we want no contraband of any kind—drugs, laundered money, weapons of mass destruction, bio- or chemical-hazards contaminating our shipments, and we certainly do not want to fathom the possibility of fouling our domestic supply chain. You do not need a very vivid imagination to know that the consequences of that would be catastrophic.

In part, some of the answers to our security concerns lie in newer developing technologies, but we must also rely on good old-fashioned common sense and American ingenuity. All stakeholders in the supply chain must closely examine their processes end to end.

I am pleased to report to you and the Committee Members today that the trade community and the U.S. Customs Service, under the direction of the Treasury Department, are working cooperatively together to improve many of the security features already in place. At the U.S. Customs Trade Symposium held last week in Washington, Customs Commissioner Bonner called upon the trade community to advance the partnership currently embracing Customs and the trade to a new plateau. Speaking on behalf of Target, COAC, and AAEI, we stand prepared to work side-by-side with Customs and other areas of the Federal Government in establishing practical, effective, and cost-efficient methods to ensure the safekeeping of our supply chain.

In my written statement submitted to the Committee, I discussed the industry partnership programs currently in place at U.S. Customs and some of the programs that Target employs to assure compliance and security. For example, Target's approved for purchase and vendor compliance programs are well positioned to complement our active participation in the Business Anti-Smuggling Coalition, otherwise known as BASC. BASC is a voluntary industry-led, Customs-supported program that was established in 1995. It was a natural evolution of the Carrier Initiative Programs launched by Customs in the late 1980's and early 1990's.

As Customs' air and sea interdiction efforts successfully closed off the smuggling corridors, the drug cartels increasingly looked for new and more innovative methods of moving their illicit products

to market. As a result, they began targeting ordinary, law-abiding, legitimate commercial cargo and the BASC program was the end result of the trade community coming together and telling the world that we do not want contraband in our shipments.

All of these programs are vigorously enforced and engaged at Target and we will be coordinating our deterrence and detection efforts throughout the company. As we speak, these programs are being strengthened and retrofitted to discourage supply chain incursions.

And so now that we may begin a lively and active dialogue on these vital matters, I relinquish the rest of my time to the Committee for questions. Mr. Chairman, thank you for allowing me to appear before you today.

Chairman LIEBERMAN. Thanks very much, Mr. Laden, a very interesting piece of the picture. That is what one of the witnesses on the first panel said. Sometimes when folks go, and unfortunately, he mentioned another store chain in Wal-Mart, but when they go into Target, they just think about the inventory coming out of the back room, but obviously a lot of it comes from all around the world and it puts you—I am fascinated that this company, Target Customs Brokers, exists, but I obviously understand why. So thanks for your testimony.

Mr. LADEN. Sure.

Chairman LIEBERMAN. Gordon Fink is President of Emerging Technology Markets and is well positioned to testify about the range of technologies that can be used either by the government or the private sector to improve security at our ports. Thanks so much for being here.

TESTIMONY OF W. GORDON FINK,[1] PRESIDENT, EMERGING TECHNOLOGY MARKETS

Mr. FINK. Thank you very much, Mr. Lieberman. I appreciate the opportunity to summarize my statement, which I ask be included in the record.

Chairman LIEBERMAN. We will do it, without objection.

Mr. FINK. Other Members of the Committee, and I applaud your holistic approach to looking at government programs. I am going to give you some personal examples from my career in the government where I can cite technology that can help out.

Technology is being used, and I will mention and highlight just a few areas. One, to improve the asset utilization of the industry, the truck tractors, the trailers, and the use of the chassis. I am going to give you some examples of that; to meet the demands of the shippers and the constant need to know where their shipment is so that they know when they can advertise—when they can start moving product into their stores.

But significantly, just recently announced by the FBI is the increase in cargo theft. This was announced by the FBI at an American Trucking Association meeting a couple months ago. It is the fastest growing crime in the United States, and they mentioned it is at $12 billion a year. A lot of that cargo theft crime goes unreported. One of the reasons is that the penalties are lax, there is a

[1] The prepared statement of Mr. Fink appears in the Appendix on page 138.

high priority or a high payment for some of the cargo value. Pentium chips are more than worth their weight in equivalent cocaine and they are not marked so it is easy to resell them. And low risk as far as the law enforcement—the risk of being caught and the penalties are not very good.

This also raises the thrust of stealing one of the trucks or one of the cargo containers even after it has arrived in the United States and use it as a delivery mechanism, as a weapon of terror. I have some ideas I will share with you about the technology that can address that.

The technology is used extensively by the truck tractors now. The long-haul trucking firms, such as Schneider, J.B. Hunt, etc., know where their tractors are, the status of the engine, the behavior of their drivers. They can remotely shut it down. But more recently, they have chosen to put in the same technology in their trailers, because that asset can be decoupled from the tractor. They need to know its status, its location, when the doors are open, when the doors are closed, and it is part of asset management as well as knowing where their cargo is.

The chassis—some on the Committee may not know what I mean by chassis, is a frame with pins on the end of it that the container sits down on and it is the device that moves a lot of these containers out of the ports, either to railheads or to their destination. There are about 750,000 of those chassis in use right now.

While Senator Collins has left—one of the things that I would like to address is the fact that electronic seals for containers is now being tested. There is a pilot program in the Northwest part of the United States where cargo entering Seattle has an electronic seal affixed to it. It is for Customs in-bond shipments that go across the border at Blaine and into Canada. The technology is starting to emerge and most of the technology is now available. I am happy to see that it is available from several different vendors so that you can start to get some competition and help make the business case in the decision to adopt the technology.

I have chosen to spend a lot of my time working with the Maritime Administration in a program they call the Cargo Handling Cooperative Program, which is described in my statement. It is a program to look for technology and make it available to the members of the industry—the carriers, the shippers, so that they can help understand what the technology is, make sure that they know what its maturity is, and then also help them make the business case for it.

Some of the technology that is very relevant is non-intrusive inspection, the so-called gamma ray inspection, which was started at the land border crossings between Mexico and the United States by U.S. Customs Service to inspect the trucks and some containers—mostly trucks and vehicles with a high degree of success. It does fit very well—with reference to some of the comments by previous panel members—to be deployed overseas at the point of embarkation.

So in addition to getting a manifest of that particular container, you can get the electronic image of it. It can be rescanned when it comes into the United States. The scanners scan so when it is in motion, not at 60 miles an hour, but roughly up to 10 miles an

hour, and it is also used on railroad trains the same way. They can rescan it to see if there has been any change. The scanning device can see if there is anything that is inconsistent with the manifest. These technologies are mature and ready for application.

I would just like to conclude by making a couple of comments. My bio mentions that I helped set up, and run the El Paso Intelligence Center for DEA. The reason it was in El Paso was to put outside of the Washington area so that we could get Customs, Coast Guard, and INS agents, along with DEA agents, to work in harmony against the drug interdiction problem. It did work and it was very highly successful, including sharing that information with State and local authorities.

There is a model that works in trying to get the different organizations to work and provide strategic intelligence—what may be coming in in what form, as well as tactical intelligence. Approximately 50 percent of the phone calls that were made by people in the field got some form of intelligence back. There was a high hit rate in the databases.

I appeared before many committees of the Congress that did not want me to merge those databases together as is now being done in the counterterrorism area. When I was with the CIA, I helped set up the Counterterrorism Center with technology support. But at the time, there was a fear of merging those databases. So we had the individual agents go into their databases, pull out what they had, and made an assessment. So we had kind of a round robin assessment and provided the information back in the field.

I also did have the pleasure, of working for Bob Ehinger, who headed the International Trade Data System activity under the Department of Treasury. One of the significant outcomes of that activity is to combine all of the information requirements of the 100-plus Federal agencies that were mentioned before into one common database so that those people that import goods into the United States only have one form to fill out. It makes the scanning, the review of that data, it was mentioned earlier, much easier to do.

So I have come here as a technologist talking about the maturity of technology, but I must also say that the response has got to be balanced by some of the other techniques, such as looking at the documentation—where that container has been, where the vessel has been, the crew on the vessel—as a part of the whole operation.

That concludes my summary.

Chairman LIEBERMAN. Thanks, Mr. Fink. That is very interesting.

Maybe I will take off from your testimony and ask the other witnesses the extent to which we are seeing some of the technologies that Mr. Fink describes embraced or utilized by the private and the public sectors, the idea of—mostly in the trucking business, but the idea that you can not only follow where the truck is, but almost what the truck driver is doing and then what is being opened and closed and when, and also this very interesting X-ray technology, which I gather lets you look inside a container——

Mr. FINK. Yes, sir.

Chairman LIEBERMAN [continuing]. To see what is there without having to open it. What is the rate of acceptance of these? Maybe

I will just go down, to the extent that you know, starting with you, Mr. Laden, in the private sector?

Mr. LADEN. The rate of acceptance is good. Some of the technology, though, is cost prohibitive still, as Mr. Fink suggested. There is an increase in availability of this kind of technology, but today, on seaborne—most of Target's business is marine.

Chairman LIEBERMAN. Right.

Mr. LADEN. On Target's business, we are not using transponders or GPS technology yet. We are using reusable seals. But we have found there is other technology or design flaws. The drug and contraband smugglers will just literally take the doors of the container off, defeating any seal that you have on, and replace the doors. We need as an industry to look at better design and what can be done.

Chairman LIEBERMAN. Mr. Acosta, are you seeing much of this new high-tech stuff coming into your work as a Customs inspector?

Mr. ACOSTA. Yes. We utilize a gamma ray machine. Our problem is, I think we have the second prototype of the gamma ray machine, so we did real good in getting in there early to get a machine, but——

Chairman LIEBERMAN. Yes.

Mr. ACOSTA [continuing]. So we have some down time with it. They are looking at it right now and hopefully we can upgrade that. We could probably use more than one, and because we have so many ports that are involved in our area, we take it on the road on occasion. So we have an opportunity to travel, for example, to the Gulf ports in Mississippi.

Chairman LIEBERMAN. And the containers go through it relatively quickly?

Mr. ACOSTA. Yes. It is funny because it is hard to—people's paradigms. So you have a truck driver and you explain that you can drive through this at about five miles an hour. It is OK. And they will drive up to a certain point and they will stop, because their idea is, well, if they are taking a picture of the container, it is going to be blurry. It is difficult to change that paradigm, but yes, you can.

Chairman LIEBERMAN. Of course, that is a great advance, because then you do not have to open it up. And the reliability, you have found, is pretty good?

Mr. ACOSTA. It is reasonably good. Our picture is very small for what we have, so it is a little more difficult. What is good for us, for example, as in the story that I told you before, we can set this up and we can run empty containers through so we do not have to pop a seal and open the door, because it will tell us for sure that a container is empty. It will tell us if there is something in the container.

Mr. FINK. I might mention, Mr. Chairman, the Port of Miami has found a lot of stolen vehicles leaving their port in what were thought to be empty containers, through X-raying empties that are departing the United States.

Chairman LIEBERMAN. Yes. That is important.

Mr. ACOSTA. We do the same thing. We have an inbound and an outbound team, and, of course, they are looking for armaments, they are looking for stolen vehicles, they are looking for currency.

So we can use that gamma ray technology both on inbound cargo and outbound cargo.

One thing I would say about containers, though, is we talk about containers and containers can simply be thought of as a box. It is no more or no less than a box that you can put things in, just like any other box. But we are talking a lot about what you might find that is put into the box, maybe something in the cargo that is put into the box or something that is thrown in along with the cargo. But along those lines, we have to remember that the box itself accounts for about half of the seizures that we make. So within the walls, in the floor, in the roofing, in the tubing that the container is constructed in, many times, that is where we find contraband hidden, and a lot can be done—there is a lot that can be hidden in the box itself without talking about the space where you store cargo.

Chairman LIEBERMAN. Thanks. Chief Cook, have you seen any of this high-tech stuff coming into use in the Port of Memphis?

Mr. COOK. Our Auto Theft Cargo Task Force has and is more and more familiar with this type of equipment every day. But usually when we come into contact with these boxes, they are already empty. We have found contraband in quite a number of them while doing other investigations, but yes, we are becoming more familiar with it every day.

Chairman LIEBERMAN. Thanks to all of you very much. I am going to call on Senator Thompson because I notice we have a vote that has just started, so I want to give my two colleagues time to ask some questions.

Senator THOMPSON. Thank you, Mr. Chairman.

I want to follow up on the technology question. I guess most people would wonder, if we have developed this technology to this advanced stage, why are we not inspecting more? What are the limits of technology? I mean, just for the layperson to understand, can scanning technology with a high degree of accuracy make a determination with regard to potential weapons of mass destruction or other things of that nature, and to what extent is it a technological limitation and to what extent is it a cost limitation?

Mr. FINK. I think it is——

Senator THOMPSON. Why are we not scanning more stuff and why do we not feel more secure if we have this capability?

Mr. FINK. One of the things is the initial cost. These systems range up to $1 million apiece, and as you get more of them in operation, that cost will go down. Then there is the person who is looking at the image. We can do a lot to make that process move into pattern recognition into the computer to assist an operator.

But there still are all deterrents, and while the payoff is high, it is not going to be 100 percent, and one of the things that we saw, of course, in the drug business and we now see in the theft business are organized criminal elements involvement. So they are very much aware and drilling out parts of the container and inserting some of their cargo in it, but you can still see some of those.

I am encouraged because the technology is proven, and I think with quantity purchases it will be deployed. As you move inspection overseas, it raises another issue. Now you are asking the port of embarkation of that container to perform the imaging. But it is

a global problem. Terrorism is a global problem. Maybe that will be part of what will help induce some of them to do it.

One other thing I would just add. I do not know if Rear Admiral Larrabee is here, but in some of the U.S. ports, they have volunteered to put some of this scanning equipment in just to keep the flow of containers going. When Customs decides to pull something, it disrupts that flow. So they have said to me, I would invest in the gamma-ray equipment in a joint project with Customs in order to keep the cargo flowing. Some of the terminals do not have a lot of land to store the cargo on when Customs decides they want to conduct inspection, they disrupt the flow. So there are a number of business factors.

Senator THOMPSON. Mr. Acosta, what would be your response to my question on why we are not inspecting more than 2 percent in some categories?

Mr. ACOSTA. Somewhat the same. The systems are very costly, and so Customs has X amount of systems. We, of course, would—ideally, if I could set it up in New Orleans, I would like to see a system up-river and one down-river—there are two separate areas that are sort of divided areas—and then another system that we could lend to some of the smaller ports, but we have one system.

The second thing is that it requires personnel to run the system. So when you set up a gamma ray machine, you have to establish the perimeter. There is an element in there that can be hazardous to individuals, so we have to be able to make sure that we have the truck run through and to set up the flow of trucks. We have to have people inside working the machine, setting the machine up. We also have to have people available who, if necessary, will open and look in the containers immediately. Some containers we will target for further examination. Others, we are so interested in the image that we are seeing, we need to get into it right away.

So that is upwards of 10 people, and I do not know if you remember, but when I told you that the personnel put in New Orleans today is 29 inspectors, that is a third of your workforce. It is very difficult. It is cost for the equipment and it is personnel. If you could give us more equipment and the personnel to operate it, we would do all of those things.

Senator THOMPSON. Why did you stop instream, or were you told to stop instream?

Mr. ACOSTA. They said it was a safety issue. I think that is bogus. I really think it is bogus.

The second thing, and I did not mention it because I was conscious of the fact that I had a small period of time to deliver the statement, the second thing is that we have been questioned recently on the number of enforcement boardings that we have determined. I guess that is a budget issue and that is a problem because we do target vessels and we are conscious of—and I worked on the task force that gave us a boarding policy 2 years ago and we are not living up to that boarding policy. As a matter of fact, it just changed.

So it bothers me that if we are true to what the policy said and we are doing vessel targeting based on all the information we had, and understand that sometimes it is difficult to get that information, that now, we have somebody that comes back and questions,

well, you have too many enforcement boardings, and I do not understand that.

Senator THOMPSON. Thank you for that. That is important.

I do want to thank Chief Cook for being here. He is responsible for the investigation of all the crimes at the international port in Memphis. You have one of the better interagency coordination groups, I think, going. You pointed out the unique circumstances there that you have to deal with. It is not only the fourth largest inland port in the country, but the second largest inland port on the shallow draft portion of the Mississippi River and serves as a transportation hub and warehouse and distribution center, and perhaps no other port in the country shares the same characteristics as Memphis.

I am wondering about a law or an approach by the Federal Government that is a one-size-fits-all. It seems to me that Memphis has some unique characteristics—inland port, heavier concentration of activity, and so forth. Do you see your situation as maybe needing some kind of different attention, than some other places?

Mr. COOK. I think it is not recognized as the port that it is. Memphis has never, until the last few years, really recognized its own potential as a distribution center, but it is growing leaps and bounds by day. In fact, I mentioned the Frank Pidgeon Industrial Park, which is a new industrial park that is being developed on the Southwest corner, just South of what is now called President's Island, and it is going to be at least half as large as the industrial complex on President's Island.

So much of the industry that I said is in Memphis, and those that come into Memphis, a large portion comes into Memphis, but it is distributed within 600 miles of Memphis. And because of the bridges, we estimated that about $2 billion worth of commerce crosses those bridges each day. We do not think that it gets enough attention as far as the types of visibility patrols.

Now, we are doing things as far as our agencies that I mentioned, Tennessee and Arkansas agencies who both join in taking care of riding on the bridges and removing vehicles and so forth on the bridges. But as far as the actual, what I think should be 24-hour marine surveillance of the bridges from below, and also attention to the barges that are so large and so potentially dangerous as far as striking the bridges and just completely removing them from the river itself.

I think that is a major concern, because one barge can actually take out both bridges, and especially from a vessel that is coming down-river. If that were to happen, it would really destroy commerce in the surrounding area. In fact, I believe it would actually kill it for at least 2 or 3 years it would take to rebuild the bridges.

Senator THOMPSON. I think you are right. A lot of people do not understand the amount of traffic and the amount of activity going on there and that makes it a port that deserves much more attention. We appreciate what you are doing there.

Mr. COOK. Thank you very much, sir.

Senator THOMPSON. We also appreciate you taking a real leadership role in terms of the Southeast in your interagency work.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Thompson.

I thank the members of this panel as well as those on the first panel. I think the Committee has learned a lot as a result of the testimony today. I would like to think about, at the next hearing on this subject, calling the heads of the Federal Government agencies involved and ask some of the same questions of them that you have raised here.

There is never enough time at these hearings, but there are a lot of questions unanswered, so I am going to leave the hearing record open for 2 weeks, and if it is all right—and even if it is not all right—we are going to submit some questions to you in writing to follow up and look forward to your answers.

In the meantime, I thank you very much for your time and the great contribution you have made. I hope we can serve as advocates for what all of you want, which is a system that is both economically productive and efficient but is also secure, most important of all.

The hearing is adjourned.

[Whereupon, at 11:58 a.m., the Committee was adjourned.]

APPENDIX

COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021

Statement of

Stephen E. Flynn, Ph.D.
Senior Fellow, National Security Studies
Council on Foreign Relations
sflynn@cfr.org
(212) 434-9676

on

"Bolstering the Maritime Weak Link"

presented before the

United States Senate
Committee on Governmental Affairs
Room 342, Dirksen Senate Office Building
Washington, D.C.

Hearing on
"Weak Links: Assessing the Vulnerability of U.S. Ports and Whether the Government is Adequately Structured to Safeguard Them"

9:30 a.m.
Thursday, December 6, 2001

Good morning, Mr. Chairman.

My name is Stephen Flynn. I am a Senior Fellow with the National Security Studies Program at the Council on Foreign Relations where I am directing a multi-year project on "Safeguarding the Homeland: Rethinking the Role of Border Controls."

It is privilege for me to be here today to testify on the vital issue of assessing the vulnerability of U.S. ports and how our government is structured to safeguard them in the wake of the tragic events of September 11. Over the past 2 ½ years, I have been conducting research that has been examining in large part the security weaknesses associated with the system of intermodal transportation that is so indispensable to support global trade and travel. That project has afforded me the opportunity to conduct field visits along the U.S.-Mexican, and U.S.-Canadian borders, within major seaports throughout the United States, in Montreal, Rotterdam, Hong Kong, and Kingston, Jamaica.

My research question has essentially been this: Given the cascading tide of peoples and goods moving through our seaports, and across our borders on trucks and trains, how do regulatory and enforcement agents accomplish their public mandates of filtering the bad from the good; and the dangerous from the benign?

The answer I have arrived at is that the U.S. government and the international community has no credible way to reliably detect and intercept illegal and dangerous people and goods that infiltrate our maritime and surface transport networks. The tools and protocols for conducting inspections, collecting and mining data, and sharing information have simply not kept pace with the size, speed, and complexity of the international networks that transport people and goods. In addition the staffing, training, and resource levels of front line agencies operating in seaports and at land border crossings are completely out of alignment with their mounting task of managing the growing threats of criminals and terrorists.

This conclusion is an extremely sobering one, particularly in light of what I argue are three unpleasant "facts of life" we must accept in the wake of the events of September 11. First, there will continue to be anti-American terrorists with global reach for the foreseeable future. Second, these terrorists will have access to the means—including chemical and biological weapons—to carry out catastrophic attacks on U.S. soil. And third, the economic and societal disruption created by the September 11 attacks and the subsequent anthrax mailings has opened a Pandora's box. Future terrorists bent on challenging U.S. power will draw inspiration from the seeming ease with which the United States can be attacked, and they will be encouraged by the mounting costs to the U.S. economy and the public psyche exacted by the hasty, ham-handed efforts to restore security.

Along with other national security experts, I belief that what we witnessed on September 11 is how warfare will be conducted in the 21st Century. What this means is that, at the end of the day if all goes well with the current fight in Afghanistan, only the terrorists of the moment will have been defeated. The United States may be unrivaled in terms of its global military, economic, and cultural reach, but there are still real limits to its power. There

will always be anarchical corners of the world, for terrorists to hide, whether in the unpoliceable areas of third world mega-cites or in the rural hideaways within failed or failing states. Even if the war on terrorism extends for a decade or more, new adversaries will arise to fill the shoes of those who have perished. Indeed, a likely consequence of the prosecution of that war will be to motivate new recruits into the ranks of terrorism. As with the drug war, "going to the source" is seductive in principle, but likely to prove illusive in practice.

Therefore, the United States and the international community face the stark reality that there will continue to be adversaries who will use catastrophic terrorism as a means of warfare. We also must be mindful of the fact that the goal of these attacks is not simply to kill people, but to create economic and societal disruption that weakens the victim and generates pressures for it to change its policies. Ultimately, therefore, a war on terrorism should be about reducing the vulnerability of the systems of transport, energy, information, finance, and labor from being exploited or targeted by terrorists.

The best way to illustrate the limits of our current security measures within seaports and the intermodal transportation networks is to consider the security challenge represented by commercial containers—the 20' and 40' boxes that are carried on ships, trains, and 18-wheelers which accounted for 80 percent of the overseas general cargo that arrived in United States in 1999—that number continues to rise and is expected to account for 100 percent of general cargo by 2010.

Consider this scenario that I posited in an article I wrote for *Foreign Affairs* a little over a year ago. Terrorists tied to Osama bin Laden might purchase a company in Karachi, Pakistan that has been in the business of sending ceramics to a New York-based importer for more than a decade. In one of the shipments they could load a chemical agent into a container ultimately destined for Newark, New Jersey, with virtually no risk that it would be intercepted. The container would likely be sent via Singapore or Hong Kong to mingle with the over one million containers that are handled by each of these ports every month. It could well be loaded aboard a 6600 TEU container ship like the *Regina Maersk*, bound for Long Beach, California which receives almost one-quarter a million containers each month. It would likely travel in-bond which means that it would not be inspected at its port of arrival. The U.S. Customs Service inspection system is built around clearing cargo at its final destination (confusingly known as the "port of entry," referring to the point at which goods enter the U.S. economy). Furthermore, the importer has up to 30 days to transport cargo from its arrival port to its port of entry. The container could be diverted or the weapon activated anywhere en route, long before its contents were subject to examination.

Now let's contemplate what the fallout might be the first time a container is used as a weapon. The American people would want to know where and how they can be assured that other containers do not pose a threat. When they learn how the maritime container trade operates, they are unlikely to be reassured. These containers can be loaded by upwards of 500,000 non-vessel operators (NVOCCs) and 40,000 freight forwarders from around the planet. After placing a numbered plastic seal on the latch of the container doors, these boxes are allowed to move into seaport terminals, aboard container ships, and on to trains and truck, with only the scantiest of information about their contents. On the infrequent occasion where

U.S. authorities examine a container—about 1 and 100 get a cursory look and roughly 1 and 500 are subjected to a comprehensive physical inspection—this is done in the port of entry.

But suppose there was a chemical weapon loaded in one of these containers which is triggered by opening its door. If this happened in the port of Newark, the effects would not be limited just to the maritime terminals within the East Coast's largest container port. The plume from a chemical weapon could readily contaminate the adjacent railroad tracks that link the northeast to the continental rail system, the New Jersey Turnpike, and the Newark International Airport—all of which are located within one mile of the container terminal. Presented with the prospect of such a calamity, government authorities might decide that no containers be allowed in the port at all. The economic consequences of cutting off the flow of cargo to a market of over 40 million consumers within a 200-mile radius are almost too-painful to contemplate, but would certainly represent an important victory for an anti-American terrorists.

I pose this dark scenario to help highlight the new security challenges associated with the post-September 11 world, and what I think represents a national and international imperative to address the issue of security within our maritime transport network. What is at stake is not just the opportunity this network presents for a terrorist who wants to exploit it so as to launch another catastrophic terrorist attack on U.S. soil. But, to a considerable extent, the fate of global trade also rests in the balance. This situation is considerably more daunting that the recent anthrax attacks. Faced with the risk of contaminated mail, we could shift to e-mail, faxes, and Fed-Ex. However, if U.S authorities find themselves having to turn off the maritime container trade spigot, we will have effectively self-imposed a blockade on our own economy. This is because there is no alternative to a container for moving general cargo between North America and Europe, Asia, Africa, and Australia.

What I have outlined above has three very important implications for the subject of today's hearing on the vulnerability of U.S. seaports and how the government is structured to the safeguard them:

(1) Seaports cannot be separated from the international transport system to which they belong. Ports are in essence nodes in a network where cargo is loaded on or unloaded from one mode—a ship—to or from other modes—trucks, trains, and, on occasion, planes. Therefore, seaport security must always be pursued against the context of transportation security. In other words, efforts to improve security within the port requires that parallel security efforts be undertaken in the rest of the transportation and logistics network. If security improvements are limited to the ports, the result will be to generate the "balloon effect"; i.e., pushing illicit activities horizontally or vertically into the transportation and logistics systems where there is a reduced chance of detection or interdiction.

(2) Port security initiatives must be harmonized within a regional and international context. Unilateral efforts to tighten security within U.S. ports without commensurate efforts to improve security in the ports of our neighbors will lead shipping companies and importers to "port-shop"; i.e., to move their business to other market-entry points where their goods are cleared more quickly. Thus the result of unilateral, stepped-up security within U.S. ports could well be to erode the competitive position of important America ports while the locus of the

security risk simply shifts outside of our reach to Canada, Mexico, or the Caribbean to ports such as Halifax, Montreal, Vancouver, and Freeport.

(3) Since U.S. ports are among America's most critical infrastructure, they should not be viewed as a primary line of defense in an effort to protect the U.S. homeland. The last place we should be looking to intercept a ship or container that has been co-opted by terrorists is in a busy, congested, and commercially vital seaport.

The fact that seaport security must be considered within a broader transportation and logistics context that includes ports outside U.S. jurisdiction has obvious implications for how the U.S. government is organized to safeguard them. Consider these important structural impediments:

(1) Agencies with responsibility for a specific transportation mode rarely communicate with their counterparts in other modes. In fact, there is a pervasive culture of competition among the modes, often reinforced by their congressional advocates, which leads to a zero-sum approach to parceling out resources. An illustration of this phenomenon is the recent decision by the House to bankroll additional airport security, in part, by diverting $60 million in supplemental monies promised to the U.S. Coast Guard to pay for its stepped-up port security mission.

(2) The security challenge associated with seaports is not just the one posed by conveyances—ships—but the operators, passengers, and cargo on those ships—and the shoreside infrastructure where those people and goods are loaded and offloaded. The federal agencies with primary oversight responsibility for the people, cargo, and conveyances are sprawled across a number of federal departments; e.g., (1) People: Consulate Affairs in the State Department and INS; (2) Goods: U.S. Customs, USDA, and FDA; and (3) Ships and the non-landside of the ports: the U.S. Coast Guard. Responsibility for landside security lies within a smorgasbord of local, state, and private entities that often differs from port to port. The thousands of trucks and their drivers that move in and out of the ports each day are perhaps the most poorly monitored and regulated of all.

(3) Since the jurisdiction of most of these agencies runs out at the water's edge, they tend to approach their regulatory and enforcement mission within a domestic framework as opposed to an international one.

This state of affairs should have been seen as unacceptable before September 11. Now there is particular urgency to taking a comprehensive approach to redressing these issues. Since, seaports are the main arteries that feed global markets by moving commodities, cargo, business travelers, and tourists, protecting that circulatory system from being compromised by terrorists is an important imperative unto itself. Enhancing transport security, therefore, is one part, about preventing terrorists from exploiting the networks to cause catastrophic harm, and the other part about sustaining the continued viability of international commerce. This task can only be accomplished by moving away from ad hoc controls at the seaports that lie within U.S. jurisdiction, and toward point of origin controls, supported by a concentric series of checks

built into the system at points of transshipment (transfer of cargo from one conveyance to another) and at points of arrival.

Moving upstream is not as difficult or futuristic of a task as it might appear at first brush. As a start, the United States and its allies should capitalize on the enormous leverage over global maritime transportation networks that a few key jurisdictions can exercise. At some point during their journey, nearly all the ships that carry general cargo must steam into or out of just a handful of global mega-ports such as Long Beach and Los Angeles, Hong Kong, Singapore, Hamburg, Antwerp, and Rotterdam. If the port authorities and their governments of just these seven ports could agree to common standards for security, reporting, and information-sharing for operators, conveyances, and cargo moving within or through those ports, those standards would become virtually universal overnight. Anyone who chose to not play by these rules would find themselves effectively frozen out of competitive access to the world's major markets.

Megaports could require, for example, that anyone who wants to ship a container through their ports, must have that container loaded in an approved sanitized facility. These facilities would have loading docks secured from unauthorized entry and the loading process monitored by camera. In high-risk areas, the use of cargo and vehicle scanners might be required with the images stored so that they can be cross-checked with images taken by inspectors at a transshipment or arrival destination.

After loading, containers would have to be fitted with a theft-resistant mechanical seal. The drivers of the trucks that deliver goods to the port would be subjected to mandatory background checks. For instance, the routes of trucks into ports could be monitored and even controlled by available technology. A microcomputer connected to a transponder and global positioning system (GPS) could be attached to the motor control system of the trucks involved, so that if they strayed out of licensed routes, the engines of the trucks would shut down and the authorities would be automatically notified. The transponder, like those used for the "E-Z-pass" toll-payment system across the northeastern United States, would give authorities the ability to monitor and control would result in an automatic alert to the police.

GPS transponders and electronic tags could also be placed on shipping container so that they could be tracked. A light or temperature sensor installed in the interior of the container could be programmed to set off an alarm if the container were opened illegally at some point during transit. Importers and shippers would be required to make this tracking information available upon request to regulatory or enforcement authorities within the jurisdictions through which it would be destined.

Manufacturers, importers, shipping companies, and commercial carriers, finally, could agree to provide to the authorities with advance notice of the details about their shipments, operators, and conveyances. This early notice would give inspectors the time to assess the validity of the data, to check it against any watch lists they may be maintaining, and provide timely support to a field inspector deciding what should be targeted for examination.

As with many safety or universal quality control standards, private trade associations could hold much of the responsibility for monitoring compliance with these security measures. As a condition of joining and maintaining membership within an association, a company would be subjected to a preliminary review of their security measures and would agree to submit to periodic and random spot checks. Without membership, access to ships servicing the mega-ports, in turn, would be denied.

This system which advances near-real time transparency of trade and travel flows would serve two purposes. First, to reduce the risk of shipments being compromised in transit. Second, to enhance the ability for enforcement officials to quickly act on intelligence of a compromise when they receive it by allowing them to pinpoint the suspected freight. The importance of achieving this second objective cannot be overstated. The sheer number of travelers and volume of trade along with the possibility of internal conspiracy even among companies and transporters who are deemed low-risk makes critical the ongoing collection of good intelligence about potential breeches in security. But, that intelligence is practically useless if it helps only to perform a post-attack autopsy. Mandating "in-transit accountability and visibility" would provide authorities with the means to detect, track, and intercept threats once they receive an intelligence alert.

Mandating that data be provided is one thing; effectively managing and mining it so as to make a credible determination of risk is another. Front-line agencies must be brought out of their 19th century stove-piped, record-keeping worlds. To reduce the potential for overload, some existing data collection requirements could be eliminated, consolidated, or accomplished by other methods such as statistical sampling. The goal should be to create within each national jurisdiction one clearing-house for receiving data about people, cargo, and conveyances. All government users of the data could then collect and analyze what they needed from that pool.

Inspectors and investigators assigned to front line regulatory and enforcement agencies will continue to play a critical role in the timely detection and interception of anomalies. To be effective, however, a serious effort must be made to improve their pay, staffing numbers, and training, and to push them beyond the border itself into common bilateral or multilateral international inspection zones. Mega-ports and regional transshipment ports should play host to these zones and allow agents from a number of countries to work side-by-side. Such an approach would take better advantage of information collected by law enforcement officials at the point of departure, allow transport-related intelligence to get into the security system sooner, and reduce the congestion caused by concentrating all inspections at the final destination. The bilateral inspection zones set up by French and British officials at both ends of the English Channel tunnel could serve as a model.

Enlisting mega-ports, focusing on point of origin security measures, and embracing the use of new technologies all support the homeland security mission be enhancing the ability of front line agencies to detect and intercept global terrorist activity before it can arrive on U.S. soil. This approach also precludes the need to impose draconian security measure within seaports that has the effect of imposing a self-embargo on the American economy. It will

require providing meaningful incentives to companies and travelers to win over their support. It mandates a serious infusion of resources to train and equip front-line agencies like Customs, INS, and Coast Guard to operate and collaborate in this more complex trade and security environment. And it involves mobilizing U.S. allies and trade partners to harmonize these processes throughout the global transportation networks.

Conclusion:

Building a credible system for detecting and intercepting terrorists who seek to exploit or target international transport networks would go a long way towards containing the disruption potential of a catastrophic terrorist act. A credible system would not necessarily have to be perfect, but it would need to be good enough so that when an attack does occur, the public deems it to be as a result of a correctible fault in security rather than an absence of security.

Ultimately getting seaport security right must not be about fortifying our nation at the water's edge to fend off terrorists. Instead, its aim must be to identify and take the necessary steps to preserve the flow of trade and travel that allows the United States to remain the open, prosperous, free, and globally-engaged societies that rightly inspires so many in this shrinking and dangerous world.

65

America the Vulnerable

Stephen E. Flynn

THE UNGUARDED HOMELAND

IT IS PAINFUL to recall that, prior to September 11, Washington's singular preoccupation when it came to protecting the U.S. homeland was national missile defense. That urgency about guarding the United States from a potential missile attack now stands in stark contrast to the government's complacency about policing America's transportation networks and land and sea borders. On September 10, just over 300 U.S. Border Patrol agents supported by a single analyst were assigned the job of detecting and intercepting illegal border crossings along the entire vast 4,000-mile land and water border with Canada. Meanwhile, after a decade of budgetary neglect, the U.S. Coast Guard, tasked with maintaining port security and patrolling 95,000 miles of shoreline, was forced to reduce its ranks to the lowest level since 1964 and to cannibalize its decades-old cutters and aircraft for spare parts to keep others operational. While debates over the merits of new missile-intercept technologies made headlines, the fact that America's terrestrial and maritime front doors were wide open did not rate even a brief mention.

Until the World Trade Center towers were reduced to rubble and the Pentagon was slashed open, most Americans, along with their government, were clearly in denial about their exposure to a terrorist attack on their own soil. Oceans to the east and west and friendly

---

STEPHEN E. FLYNN is Senior Fellow in the National Security Studies Program at the Council on Foreign Relations and a Commander in the U.S. Coast Guard. This article is adapted from his chapter in *How Did This Happen? Terrorism and the New War*, published by PublicAffairs and *Foreign Affairs* with the support of the Council on Foreign Relations.

continental neighbors to the north and south had always offered a healthy measure of protection. And Americans have generally disapproved of extensive efforts at domestic security. They were willing to staff and bankroll the defense and intelligence communities to contain the Soviet Union and to deal with conflicts "over there," but the quid pro quo was supposed to allow civilians at home to enjoy the full extent of their accustomed freedoms.

As Americans now contemplate the road ahead, they need to accept three unpleasant facts. First, there will continue to be anti-American terrorists with global reach for the foreseeable future. Second, these terrorists will have access to the means—including chemical and biological weapons—to carry out catastrophic attacks on U.S. soil. And third, the economic and societal disruption created by both the September 11 attacks and the subsequent anthrax mailings will provide grist for the terrorist mill. Future terrorists bent on challenging U.S. power will draw inspiration from the seeming ease with which the United States can be attacked, and they will be encouraged by the mounting costs to the U.S. economy and the public psyche exacted by the hasty, ham-handed efforts to restore security.

STOPPING THE PENDULUM

THE CAMPAIGN in Afghanistan has commanded the bulk of the waking moments of the senior leadership at the White House, the Pentagon, and the State Department. But at the end of the day, even if all goes well in this fight, only the terrorists of the moment will have been defeated. Places will always exist for terrorists to hide, especially before they have committed large-scale atrocities, and new adversaries will eventually arise to fill the shoes of those who have perished. As with the war on drugs, "going to the source" is seductive in principle but illusive in practice.

Focusing exclusively on the current terrorist hunt, moreover, takes precious time and political capital away from confronting perhaps the most serious danger emanating from the September 11 attacks: the exposure of the soft underbelly of globalization. The very same system that fueled the glory days of the 1990s—the openness of the U.S. economy to the world, which helped spawn unparalleled

growth—also increased America's vulnerability. For years U.S. policymakers, trade negotiators, and business leaders have operated on the naive assumption that there was no downside to building frictionless global networks of international trade and travel. "Facilitation" was the order of the day. Inspectors and agents with responsibility for policing the flows of people and goods passing through those networks were seen as nuisances at best—and at worst, as barriers to competitiveness who should be marginalized, privatized, or eliminated wherever possible.

By the afternoon of September 11, however, the pendulum had swung the other way. The attackers had hijacked four domestic airliners. Federal authorities nevertheless immediately ordered the closing of U.S. airspace to all flights, both foreign and domestic, shut down the nation's major seaports, and slowed truck, car, and pedestrian traffic across the land borders with Canada and Mexico to a trickle. This draconian response reflected an appropriate lack of confidence in the routine measures used for filtering the dangerous from the benign in the cross-border flows of people, cargo, and conveyances. Nineteen men wielding box-cutters ended up accomplishing what no adversary of the world's sole superpower could ever have aspired to: a successful blockade of the U.S. economy.

Luckily, an alternative exists between maintaining trade and travel lanes so open that they practically invite terrorists to do their worst, and turning off the global transportation spigot whenever a terrorist attack occurs or a credible threat of one arises. It is possible to keep global commerce flowing while still putting in place systems that reduce risk. But the first step has to be an acknowledgment that we have been sold a bill of goods by the purveyors of a "less-is-more" approach to managing globalization. Global integration will be sustainable, we now know, only if systems for regulating and policing it keep improving as well.

Governments around the world that share an interest in sustaining the free flow of people, goods, capital, and ideas must be encouraged to develop and enact common preventive and protective measures to facilitate legitimate cross-border movements while stopping illegitimate and dangerous ones. Washington has the leverage necessary to gain support for such a process, since all roads lead to and from U.S. markets.

It must now put that leverage to good use. Most of the owners, operators, and users of the global transportation networks are in the private sector, however, and they must also be enlisted in any effort to enhance security and controls. The result will be an imperfect system but one that will do a much better job at controlling the risks and consequences of catastrophic terrorist attacks than do the arrangements prevailing now.

THE SHIPPING NEWS

THE WORLD was understandably shocked by the carnage and the audacity of the September 11 attacks. But the aftermath may have been almost as distressing. Americans who had felt invulnerable discovered that their government had been lax in detecting and intercepting terrorists alighting on U.S. shores. Queasiness about border control and transport-security measures quickly spread to include many of the systems that underpin the U.S. economy and daily life. Suddenly guards were being posted at water reservoirs, power plants, and bridges and tunnels. Maps of oil and gas lines were removed from the Internet. In Boston, a ship carrying liquefied natural gas, an important source of fuel for heating New England homes, was forbidden to enter the harbor because local fire officials feared that, if targeted by a terrorist, it would create a destructive bomb that could lay low much of the city's densely populated waterfront. An attack on a driver by a knife-wielding lunatic on a Florida-bound Greyhound bus led to the immediate cessation of the entire national bus service and the closing of the Port Authority Bus Terminal in New York City. Agricultural crop-dusting planes were grounded out of concern that they could be used to spread chemical or biological agents.

As Americans continue their ad hoc post–September 11 domestic security survey, they will likely be horrified by what they find. The competitiveness of the U.S. economy and the quality of life of the American people rest on critical infrastructure that has become increasingly more concentrated, more interconnected, and more sophisticated. Almost entirely privately owned and operated, the system has very little redundancy. But most of the physical plant, telecommunications, power, water supply, and transportation infrastructure

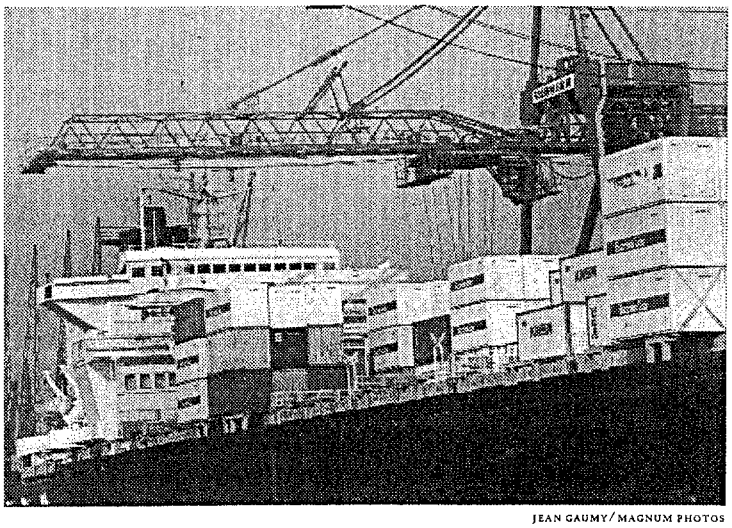
on U.S. territory lies unprotected or is equipped with security sufficient to deter only amateur vandals, thieves, or hackers. For terrorists interested in causing mass disruption, these vulnerable networks present extremely attractive targets.

The problem, however, is not just that the United States offers an almost limitless menu of enticing targets. It is that the existing border-management architecture provides no credible means for denying foreign terrorists and their weapons entry into the United States to get access to these targets. Given the limited staff and tools border inspectors have to accomplish their mission, they face horrific odds. In 2000 alone, 489 million people, 127 million passenger vehicles, 11.6 million maritime containers, 11.5 million trucks, 2.2 million railroad cars, 829,000 planes, and 211,000 vessels passed through U.S. border inspection systems. And the majority of this traffic was concentrated in just a handful of ports and border crossings. One-third of all the trucks that enter the United States annually, for example, traverse just four international bridges between the province of Ontario and the states of Michigan and New York.

The U.S. economy rests on a virtually endless menu of attractive targets for terrorists.

The rule of thumb in the border-inspection business is that it takes five inspectors three hours to conduct a thorough physical inspection of a loaded 40-foot container or an 18-wheel truck. Even with the assistance of new high-tech sensors, inspectors have nowhere near the time, space, or personnel to inspect all the cargo arriving. A case in point is the Ambassador Bridge between Detroit, Michigan, and Windsor, Ontario. There, at the world's busiest commercial land-border crossing, nearly 5,000 trucks entered the United States each day in 2000. With only 8 primary inspection lanes and a parking lot that can hold just 90 tractor-trailers at a time for secondary or tertiary inspections, U.S. Customs officers must average no more than two minutes per truck. If they fall behind, the parking lot fills, trucks back up onto the bridge, and the resulting pileup virtually closes the border, generating roadway chaos throughout metropolitan Windsor and Detroit.

The loads these trucks carry are mostly low-risk shipments of auto parts and materials, but a substantial amount of the cross-border



JEAN GAUMY/MAGNUM PHOTOS

No entry? Shipping containers in transit

cargo with Canada originates overseas. One half of the one million containers arriving in the Port of Montréal each year, for instance, is destined for the northeastern or midwestern United States. In trying to figure out whether these containers might pose a risk, Canadian inspectors have little to go by. The cargo manifest provides only the sketchiest of details about a container's contents and in many cases includes no information about the original sender or the ultimate customer. To get more information, inspectors must engage in the labor-intensive and time-consuming act of tracking down shipping intermediaries, who are often difficult to reach.

Moreover, whether a container arrives in the United States through Canada or directly from Europe or Asia, it is unlikely to be examined when it first arrives on U.S. soil. The U.S. Customs Service inspection system is built around clearing cargo not at its arrival port but at its final destination (confusingly known as the "port of entry," referring to the point at which goods enter the U.S. economy). Chicago, for example, is the nation's fourth-largest port of entry. An importer operating there can count on Customs officers' never reviewing the cargo manifest until after a container has reached the city itself, even though the shipment may have actually entered the United States

through Los Angeles, Miami, or the St. Lawrence Seaway. Furthermore, the importer has up to 30 days to transport cargo from its arrival port to its port of entry. At any given time, therefore, U.S. authorities are not in a position to verify the contents or senders of thousands of multi-ton containers traveling on trucks, trains, or barges on U.S. roads, rails, and waterways through America's heartland.

MALIGN NEGLECT

THE REMARKABLE ADVANCES in U.S. economic competitiveness over the last decade are rooted in the very openness and efficiency that have permitted people and commerce to flow so readily within and across U.S. borders. Modern businesses have capitalized on improvements in the timeliness and reliability of transport by constructing global assembly lines centered around outsourcing contracts. At the same time, managers have squeezed inventory stocks to reduce overhead costs. Traditionally, companies could ensure their ability to meet customers' demands by relying on internal production or well-stocked shelves. The advent of "just-in-time" delivery systems, however, has lowered the need to carry such insurance and has allowed corporations such as Wal-Mart to become enormously profitable.

Not surprisingly, many private-sector actors have not been fans of the administrative and inspection work of regulatory and enforcement officials charged with overseeing the people, conveyances, and cargo arriving at U.S. borders or moving through global transport networks. The pervasive view among many in the private sector has been that more inspectors mean more inspections, which translates into slower shipments. Accordingly, the growth in the volume and velocity of cross-border trade has generated little political support for a commensurate growth in the staffing, training, and equipping of the agencies responsible for providing security. Instead, those agencies have been starved of personnel, forced to work with obsolete data-management systems, and even, thanks to congressional pressure, subjected to performance sanctions if they disrupt the flow of commerce by making anything more than token random spot-checks.

Even as U.S. trade with Canada climbed from $116.3 billion in 1985 to $409.8 billion in 2000, for example, the number of Customs

inspectors assigned to the northern border decreased by roughly one-quarter. Prior to September 11, half of the primary inspection booths at the border crossings in the states of Washington, Montana, North Dakota, Minnesota, Michigan, New York, Vermont, and Maine routinely remained closed because no one was there to staff them. And those inspectors working the booths that were open were evaluated in part by how well they met "facilitation" performance standards designed to reduce waiting times.

> The only surprise is that the United States managed to dodge the terrorism bullet for so long.

The world may be well into the electronic age, but the U.S. Customs Service is still struggling with paper-based systems. For years its proposed Automated Commercial Environment and International Trade Data System projects have run aground on the twin shoals of flat federal budgets and industry disputes over the timing, format, and quantity of commercial data to provide to Customs in advance. It was only in April 2001 that the Customs Service received the seed money to get started on these projects, which it projects will take years to develop and implement. In the interim, inspectors will have to rely on only the bluntest of data-management tools.

If the data-management and data-mining situation is grim for Customs, it is even grimmer for other front-line agencies such as the Coast Guard, the Immigration and Naturalization Service (INS), and the Department of Agriculture, all of whose officers desperately need communication and decision-support tools to carry out their jobs. But even if these agencies did join the information age, they would still face bureaucratic and legal barriers that currently hinder them from talking with one another.

For example, consider the case of a ship with a shadowy record of serving in the darker corners of the maritime trade. Its shipping agent sends notice that it will be importing a type of cargo that does not square with its home port or its recent ports of call. Some of its crew are on an intelligence watch list because they are suspected of having links with radical Islamist organizations. And the ship is scheduled to arrive on the same day as a tanker carrying highly volatile fuel. The U.S. public might reasonably expect that with a shady past, suspect

cargo, questionable crew, and clear target of opportunity, such a ship would be identified, stopped, and examined before it could enter U.S. waters. The odds of such an interdiction happening are slightly better now than prior to September 11, but there remain significant structural hurdles to anyone's being able to see all the red flags simultaneously.

The Coast Guard would be likely to know something about the ship itself and about the scheduled arrival of a tanker carrying hazardous cargo. The Customs Service might have some advance cargo manifest information (although if a ship is carrying bulk materials, this information is typically not collected until after the ship gets to its arrival port). The INS should know something about the crew, but its information is likely to arrive in a fax and must be manually entered into its computers by an agent. None of the front-line inspectors in these agencies, meanwhile, is likely to have access to intelligence from the FBI or the CIA. None of them, therefore, would see the whole picture or pass on his or her information to somebody who would. And in today's system, all of the agencies face far more potentially suspect people, cargoes, and ships than they can ever manage to inspect.

THE PRICE OF HOMELAND INSECURITY

GIVEN the disgraceful neglect of front-line regulatory and law enforcement agencies, the surprise is not that the attacks of September 11 took place; it is that the United States managed to dodge the catastrophic terrorism bullet for so long. Now that this sad precedent has been set, however, improving the capability to detect and intercept terrorists or the means of terrorism heading for U.S. shores is even more critical than before, for three reasons.

First, the absence of a credible capacity to filter illicit cross-border activity will carry a high price tag in a newly security-conscious world. The automotive industry offers a simple example. Just 36 hours after the September 11 attack, DaimlerChrysler announced that it would have to close one of its assembly plants because Canadian supplies were caught in an 18-hour traffic jam at the border. Ford then announced that five of its assembly plants would have to lie idle the following week. The cost of this loss in productivity? Each assembly plant produces on average $1 million worth of cars per hour.

In the future, not only will the risk of another attack be higher but the number of threats and warnings that must be taken seriously will increase dramatically. U.S. policymakers may thus find themselves routinely compelled to order up a transportation quarantine as a preventive measure to protect the homeland. The costs are difficult to calculate, but they are sure to take a toll on international trade and U.S. competitiveness. Companies have made massive capital outlays in technology and infrastructure to leach as much uncertainty and friction as possible from the logistics and transportation networks. Now they may see the expected savings and efficiencies from their investments in just-in-time delivery systems go up in smoke.

The political and diplomatic costs of not getting border management right, meanwhile, will also be painfully high. If U.S. policymakers believe the chances of detecting and intercepting terrorist attacks are small, they may feel compelled to rush into foreign counterterrorist operations that are ill-advised or premature. The price of securing foreign cooperation in these efforts—often some form of diplomatic concession or averted eyes—could prove high in the long run. So restoring a sense that terrorist threats to the United States can be managed, thus giving Washington the breathing room to make considered choices about counterterrorism policy, is important.

Finally, a sense of defeatism about the possibility of stopping terrorism places a heavy burden on domestic policing and civil defense. If the assumption is that terrorists will always be able to slip through the border and set up shop on U.S. soil, then the argument for allowing law enforcement and intelligence agencies to conduct increasingly more intrusive domestic surveillance becomes compelling. Giving up on border management could also lead to the imposition of an extremely costly "security tax" on significant areas of national life.

FILTERING BAD FROM GOOD

INTERNATIONAL transportation networks are the arteries that feed global markets by moving commodities, cargo, business travelers, and tourists. Protecting that circulatory system from compromise by terrorists is an imperative unto itself, even if an adversary or a weapon of mass destruction could find an alternative way into U.S. territory.

In fact, this task deserves top billing over other, competing defensive measures such as constructing a missile defense system. If a missile were fired at a U.S. city and it could not be intercepted, it could cause horrible destruction and mass casualties. But if a weapon of mass destruction were loaded on a boat, truck, train, or maritime container and set off in a congested seaport, on a bridge during rush hour, or downtown in a major urban center, the results would be even worse. In addition to the local destruction and casualties, such an attack would expose the lack of credible security within the country's transportation networks and bring them to a complete standstill. The first scenario would involve damage caused by the adversary; the second would include both the damage caused by the adversary and the costs associated with a self-applied tourniquet to our global transport lifelines.

Enhancing security for transportation networks, therefore, is partly about preventing terrorists from exploiting those networks and partly about sustaining the continued viability of international commerce. The authorities can accomplish this task by moving from ad hoc controls at the borders of individual countries toward point-of-origin controls, supported by a concentric series of checks at points of transshipment (transfer of the cargo from one conveyance to another) and at points of arrival. This more comprehensive system is particularly important for the United States, where trying to distinguish the illicit from the licit at the border or within ports is like trying to catch minnows at the base of Niagara Falls.

Moving upstream is not as difficult or futuristic a task as it might appear. As a start, the United States and its allies should capitalize on the enormous leverage over global transportation networks that just a few key jurisdictions exercise. The overwhelming majority of trade moves by sea, and at some point during its journey nearly all the ships that carry it must steam into or out of just a handful of global megaports such as Long Beach and Los Angeles, Hong Kong, Singapore, Hamburg, Antwerp, and Rotterdam. If the port authorities and governments responsible for just these seven ports could agree to common standards for security, reporting, and information-sharing for operators, conveyances, and cargo, those standards would become virtually universal overnight. Anyone who chose to not play by those rules would be effectively frozen out of competitive access to the world's major markets.

Megaports could require, for example, that anyone who wants to ship a container through them must have that container loaded in an approved, security-sanitized facility. These facilities would have loading docks secured from unauthorized entry and the loading process monitored by camera. In high-risk areas, the use of cargo and vehicle scanners might be required, with the images stored so that they could be cross-checked with images taken by inspectors at a transshipment or arrival destination.

After loading, containers would have to be fitted with a theft-resistant mechanical seal. The drivers of the trucks that deliver goods to the port would be subjected to mandatory background checks. Jacob Schwartz, a professor of mathematics and computer science at New York University, has suggested that the routes of trucks into ports could be monitored and even controlled by available technology. A microcomputer connected to a transponder and global positioning system (GPS) could be attached to the motor control system of the trucks involved, so that if they strayed out of licensed routes their engines would shut down and the authorities would be automatically notified. The transponder, like those used for the "E-Z Pass" toll-payment system across the northeastern United States, would give authorities the ability to monitor and control each vehicle's movements, and it would be programmed so that tampering with it would result in an automatic alert to the police.

GPS transponders and electronic tags could also be placed on shipping containers so that they could be tracked. A light or temperature sensor installed in the interior of the container could be programmed to set off an alarm if the container were opened illegally at some point during transit. Importers and shippers would be required to make this tracking information available upon request to regulatory or enforcement authorities within the jurisdictions through which their cargo would move or toward which it would be destined.

Manufacturers, importers, shipping companies, and commercial carriers, finally, could agree to provide authorities with advance notice of the details of their shipments, operators, and conveyances. This early notice would give inspectors time to assess the validity of the data, check it against any watch lists they may be maintaining, and provide support to a field inspector deciding what should be targeted for examination.

As with many safety or universal quality-control standards, private trade associations could hold much of the responsibility for monitoring compliance with these security measures. As a condition of joining and maintaining membership within an association, a company would be subjected to a preliminary review of its security measures and would agree to submit to periodic and random spot checks. Without membership, access to ships servicing the megaports, in turn, would be denied.

To confirm the legal identity and purpose of international travelers, off-the-shelf technologies could be readily embraced to move away from easily forgeable paper-based documents such as visas or passports. Governments could embrace universal biometric travel identification cards that would contain electronically scanned fingerprints or retina or iris information. These ATM-style cards would be issued by consulates and passport offices and presented at the originating and connecting points of an individual's international travel itinerary. Airports, rail stations, rental car agencies, and bus terminals could all be required to install and operate card readers for any customers moving across national jurisdictions. Once entered, electronic identity information would be forwarded in real time to the jurisdiction of the final destination. The objective would be to provide authorities with the opportunity to check the identity information against their watch lists. If no red flags appeared, it would not be necessary to conduct a time-consuming and intrusive search. For noncitizens, a country could also require the presentation of these cards for renting cars, flying on domestic flights, or using passenger rail service.

Many border-control agencies are still using nineteenth-century means for collecting and storing data.

Mandating that data be provided is one thing; effectively managing and mining it so as to make a credible determination of risk is another. Front-line agencies must be brought out of their stovepiped, nineteenth-century record-keeping worlds. To reduce the potential for overload, some existing data collection requirements could be eliminated, consolidated, or accomplished by other methods, such as statistical sampling. The goal should be to create within each national jurisdiction

one clearing-house for receiving data about people, cargo, and conveyances. All government users of the data could then collect and analyze what they needed from that pool.

Inspectors and investigators assigned to border-control agencies will continue to play a critical role in the timely detection and interception of anomalies. To be effective, however, a serious effort must be made to improve their pay, staffing numbers, and training, and to push them beyond the border itself into common bilateral or multilateral international inspection zones. Megaports and regional transshipment ports should play host to these zones and allow agents from a number of countries to work side by side. Such an approach would take better advantage of information collected by law enforcement officials at the point of departure, allow transport-related intelligence to get into the security system sooner, and reduce the congestion caused by concentrating all inspections at the final destination. The bilateral inspection zones set up by French and British officials at both ends of the English Channel tunnel could serve as a model.

RETHINKING HOMELAND SECURITY

As the nineteenth-century Prussian military theorist Karl von Clausewitz famously noted, "war is not an independent phenomenon, but the continuation of politics by other means." At its heart, therefore, an appropriate response to the kind of asymmetric warfare that catastrophic terrorism represents must weaken its political value for an adversary. If an attack, even on the scale of those carried out on September 11, fails to translate into any tangible change in U.S. power or policies, than it becomes only a contemptible act of mass murder and high-end vandalism. Of course, a few evil people will still remain willing to commit such crimes. But a terrorist who concludes that the business of America will continue unabated despite an attack on U.S. soil will likely find little value in launching such an attack.

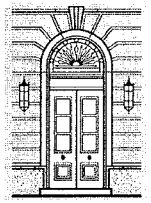
Building a credible system for detecting and intercepting terrorists who seek to exploit or target international transport networks would go a long way toward containing the disruptive potential of a catastrophic terrorist act. A credible system would not necessarily have to be perfect, but it would need to be good enough so that when an attack

does occur, the public deems it to be the result of a correctable fault in security rather than an absence of security.

Such a system, however, must extend beyond U.S. borders. Washington must move quickly beyond the Bush administration's initial steps in this area, which seem based on a mission of homeland security seen largely through the prism of civil defense. If America's future safety and prosperity were tied only to infrastructure located on U.S. soil, then a White House Office of Homeland Security dedicated to herding federal, state, and local bureaucratic officials might be appropriate. In fact, however, the United States depends on infrastructure that spans the globe.

Reducing the risk and consequences of attacks directed against the United States, therefore, cannot be accomplished simply by tweaking the roles and capabilities of agencies whose writ runs only to the nation's shores. Better preparedness and coordination of domestic agencies is important and necessary, but it is not sufficient. And the same is true for military and diplomatic campaigns overseas to root out international terrorism at its source. Manhunts carried out by U.S.-led international posses will continue to be an essential weapon in the counterterrorism arsenal. But the more daunting challenge will be to reduce the vulnerability of the systems of transport, energy, information, finance, and labor.

The massive post–September 11 outpouring of public and international support for combating terrorism will inevitably wane. This makes it all the more urgent to begin the painful process of fundamentally reforming border-management practices so that good and bad flows can be distinguished from one another and treated appropriately. Ultimately, getting homeland security right is not about constructing barricades to fend off terrorists. It is, or should be, about identifying and taking the steps necessary to allow the United States to remain an open, prosperous, free, and globally engaged society.

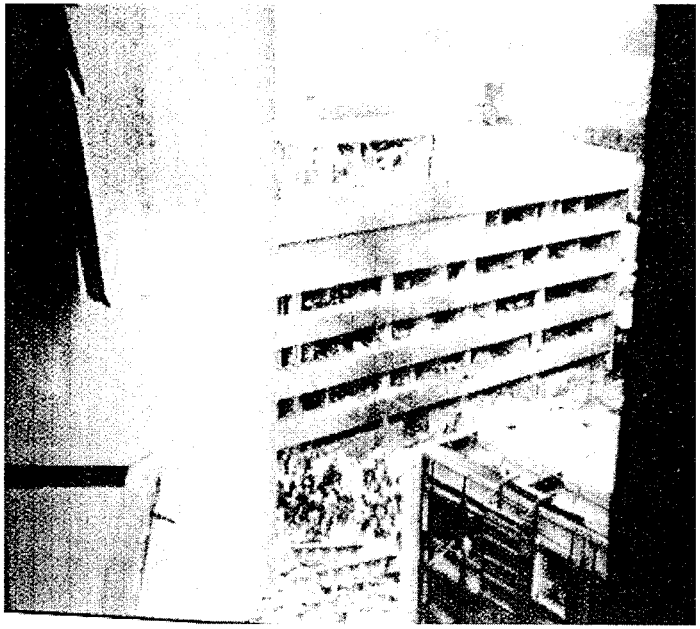


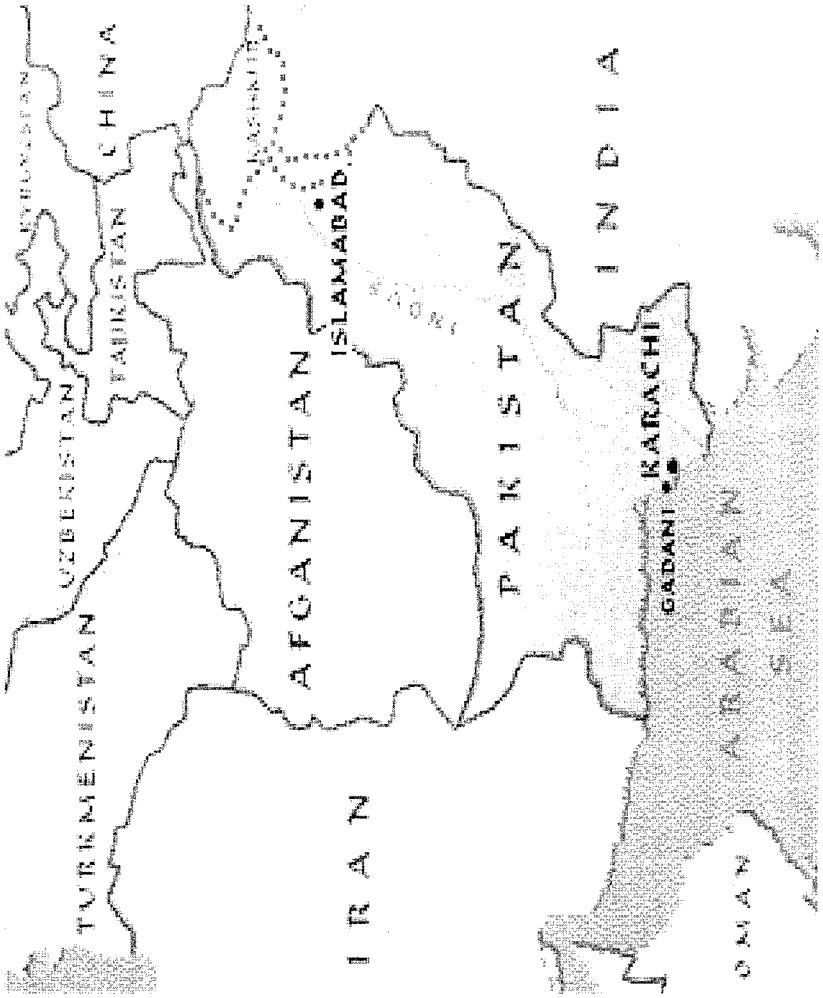
THE COUNCIL ON FOREIGN RELATIONS

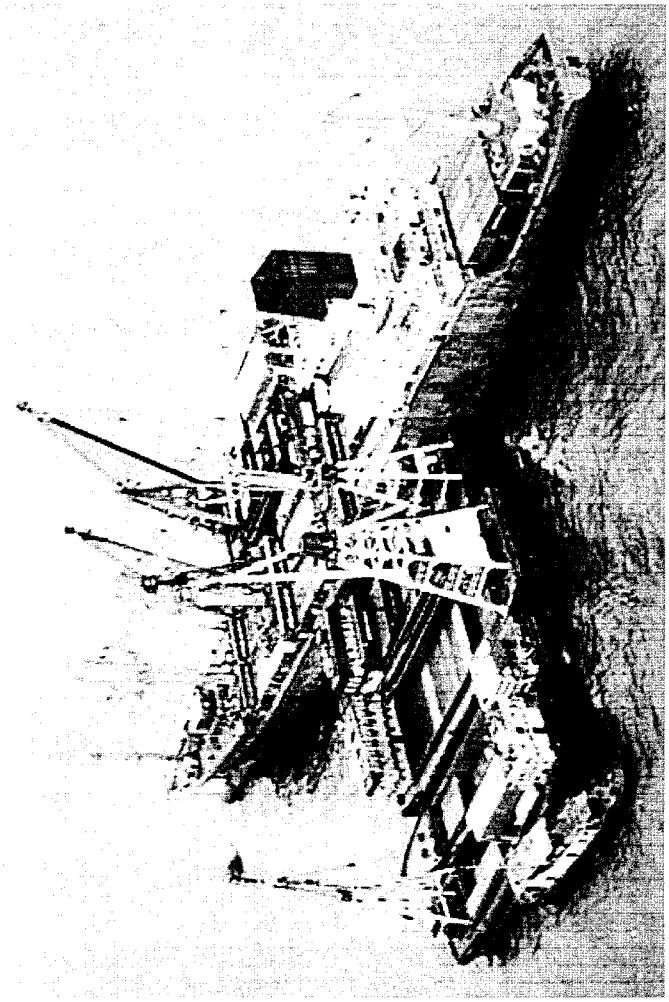
"Bolstering the Maritime Weak Link"

Stephen E. Flynn, Ph.D,
Senior Fellow, National Security Studies
Council on Foreign Relations
sflynn@cfr.org

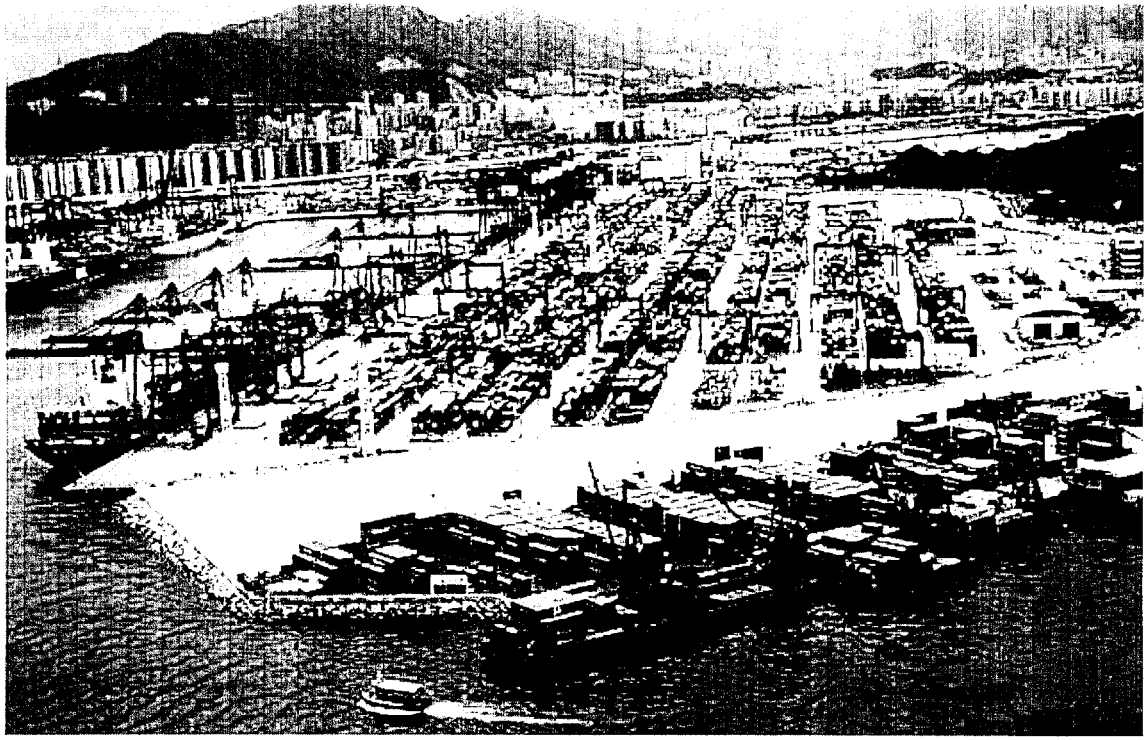
USAMA BIN LADEN

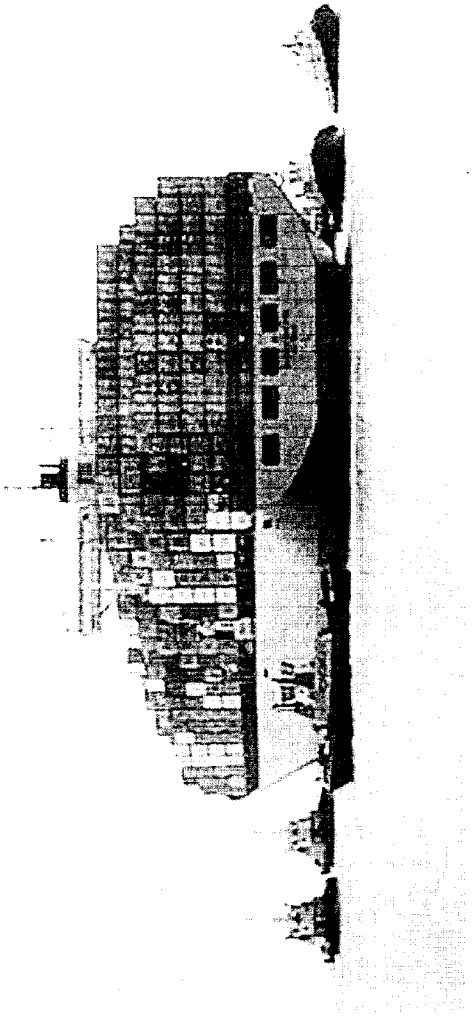


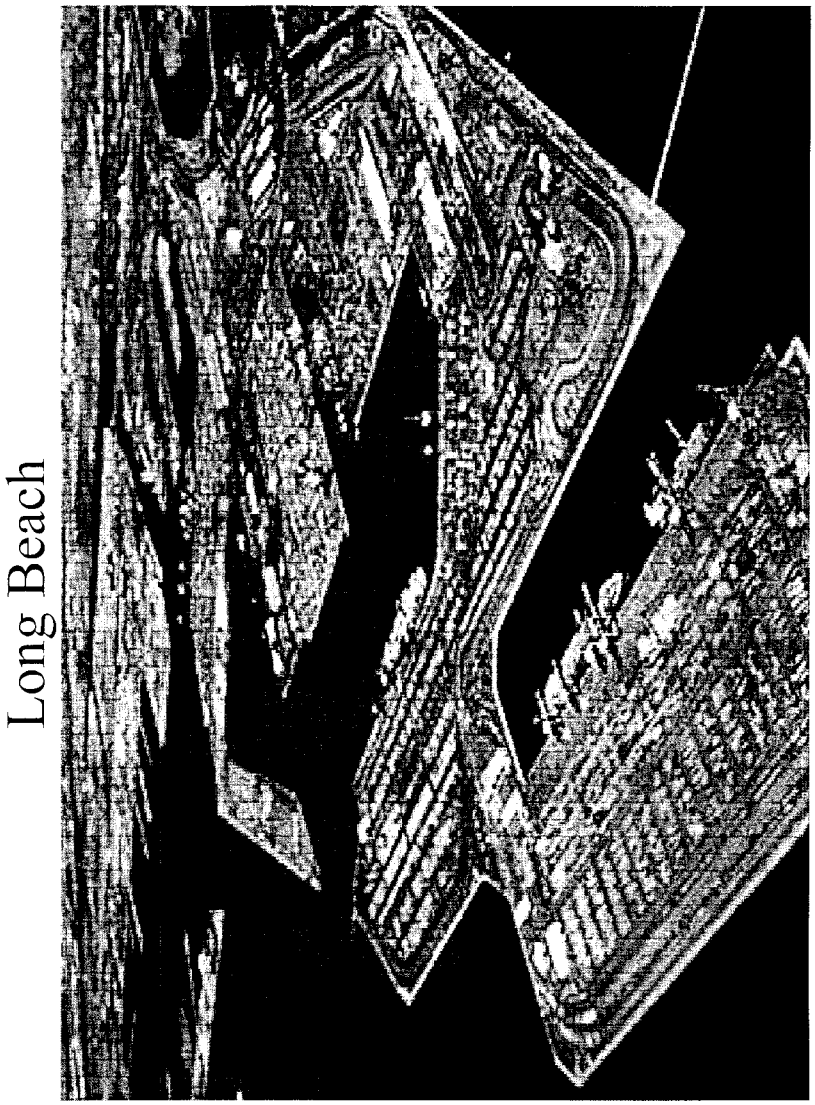

TURKMENISTAN
UZBEKISTAN
TAJIKISTAN
CHINA
AFGANISTAN
ISLAMABAD
IRAN
PAKISTAN
INDIA
KARACHI
GADANI
ARABIAN
SEA
OMAN



Container Pier in Hong Kong






Long Beach

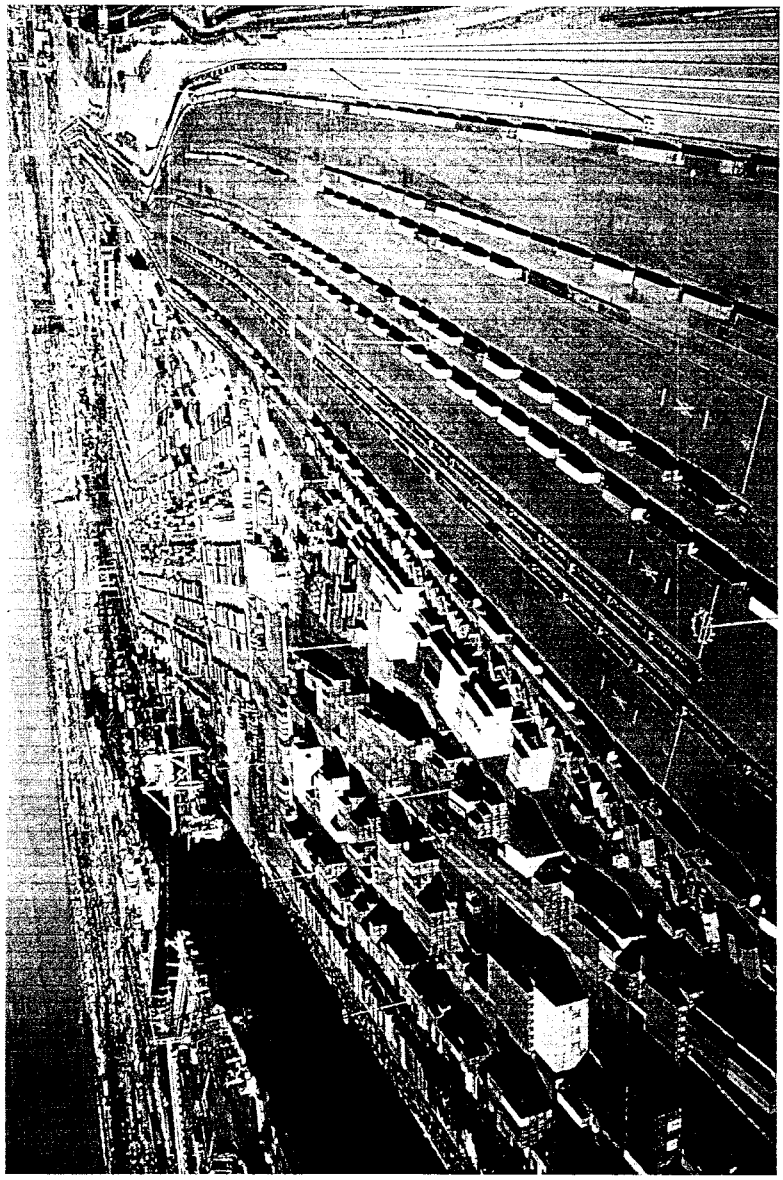
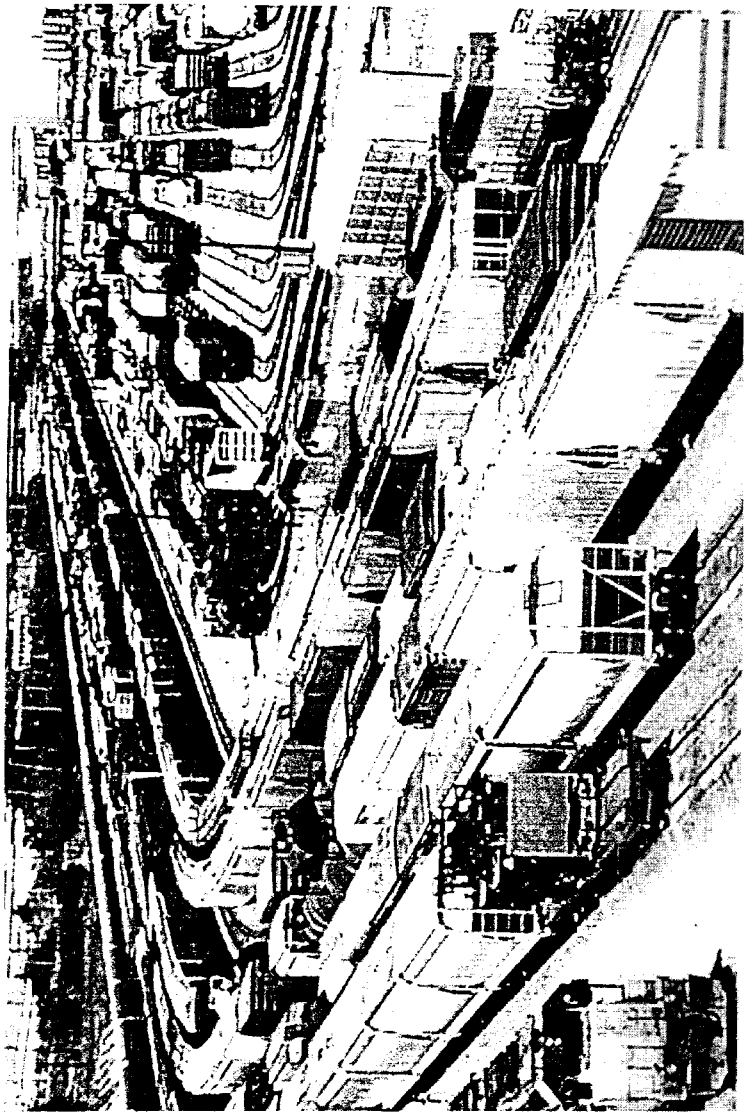
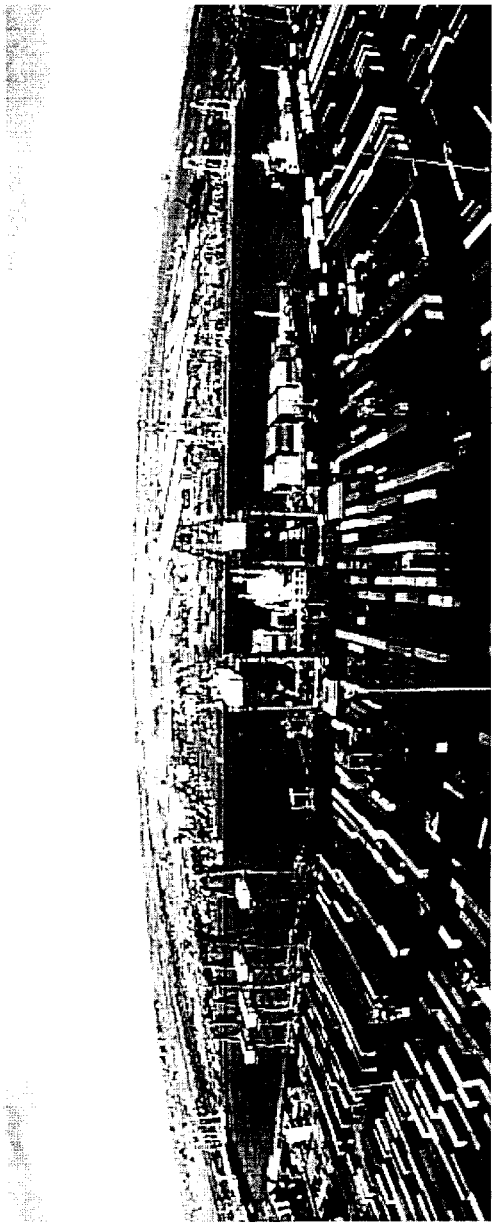
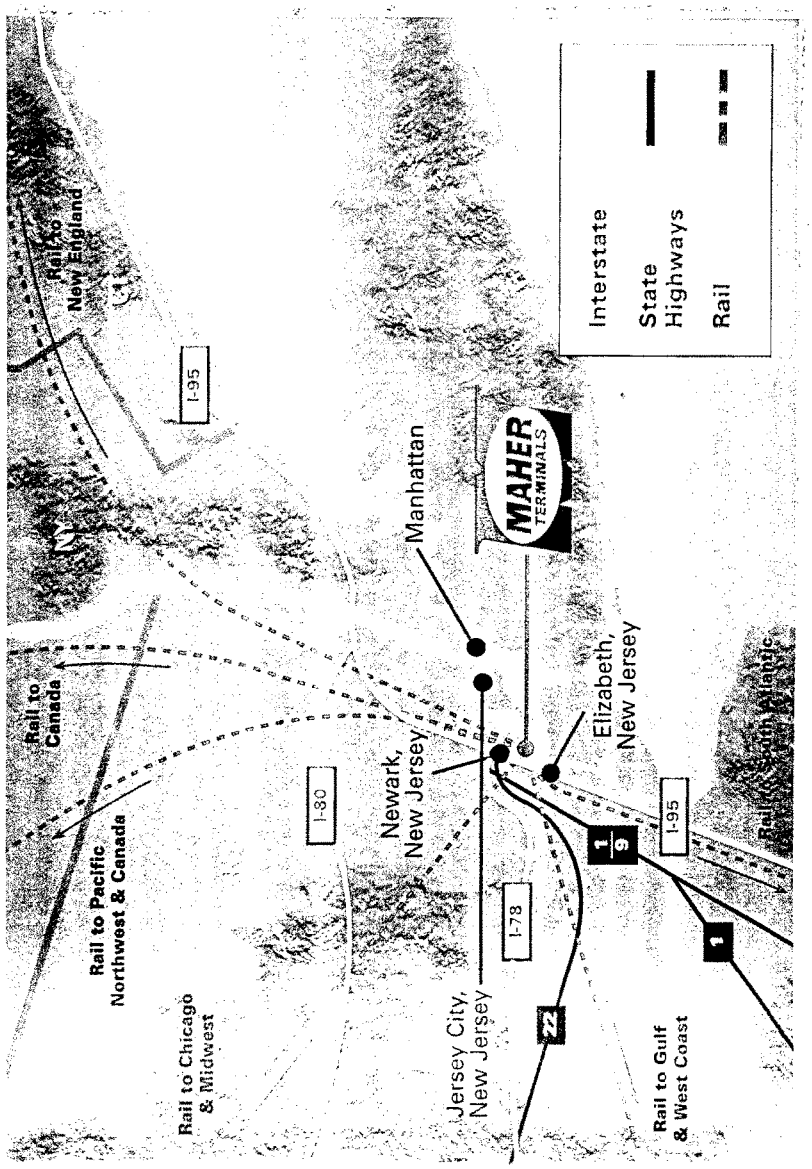


Photo ©1997 by Stanley S. Brandt






Rail to Canada
Rail to Pacific Northwest & Canada
Rail to Chicago & Midwest
Rail to New England
I-95
I-80
I-78
Newark, New Jersey
Jersey City, New Jersey
Manhattan
MAHER TERMINALS
Elizabeth, New Jersey
22
1/9
1
I-95
Rail to Gulf & West Coast
Interstate
State Highways
Rail

Testimony of F. Amanda DeBusk
Before the Senate Committee on Governmental Affairs
December 6, 2001

I am honored to be here today. I am speaking to you as a former Commissioner on the Interagency Commission on Crime and Security in U.S. Seaports. President Clinton established the Commission by Executive Memorandum on April 27, 1999. Sen. Bob Graham was instrumental in the Commission's establishment. I served on the Commission as the Commerce Department representative in my capacity as Assistant Secretary for Export Enforcement. The Commission issued a report in August 2000 with 20 findings and recommendations. I would like to highlight those that are most important for this Committee post September 11.

Let me provide some background. One of the underlying concerns was how wide open our seaports are compared to our airports. In most cases, there is free access to the seaports. The Commission found that significant criminal activity was taking place at most of the 12 seaports surveyed. At many seaports, it is legal to carry firearms, so criminals with arms may have access to terminals where passengers embark for cruises. Concerning cargo, because of misreporting and lack of reporting, no one knows in a timely fashion, if ever, what is in those containers at our seaports. One of the cases my former office investigated involved a riot control vehicle that was exported to China as a fire truck. The vehicle resembled a tank and had a turret for spraying pepper gas. It

was exported in a container, and no one knew at the time of export what was inside.

The Commission approached the crime and security problem with the possibility of terrorist activity associated with the New Millennium. Thankfully, nothing happened.

At that time, the FBI considered the threat of terrorism directed at any U.S. seaport to be low. However, even though the threat was low, the FBI considered that our vulnerability to attack was high. The Commission found that the state of security at seaports generally ranged from poor to fair, with a few exceptions where the security was good.

Today, I would like to highlight recommendations in four areas relevant to this Committee: enhanced interagency coordination, physical security at the ports, better and more timely information about cargo transitting the ports, and increased use of technology.

First, we need better interagency coordination. There are 361 seaports. Most ports are chartered by states or local government. Some terminals are operated by public port authorities; others are private. There is no central federal authority. There are at least 15 federal agencies with jurisdiction at the seaports. In addition, there are state and local agencies and the private sector. Every single group is important for combating terrorism and has something to contribute. Coordinating these groups is a monumental undertaking. Perhaps a Department of National Homeland Security could play a leadership role in this coordination.

The Commission found that there needed to be a comprehensive and definitive statement of federal responsibility. The federal government needs to conduct threat assessments to determine where the threat is greatest and where we urgently need preventive measures. The federal government should strengthen coordination to more effectively address terrorism. It should work with all stakeholders. Key information available to the federal government should be disseminated to others as needed.

Let me provide an example of where better coordination would be useful. The FBI has excellent regional counterterrorism task forces that consist of federal, state and local agencies. However, they did not focus on the seaports at the time of our study. They should do so.

S. 1214, an amendment to the Merchant Marine Act, has some good proposals on establishing local port security committees.

Second, the Commission found that we need better physical security at the seaports for both vehicles and people. At many ports, access is virtually uncontrolled. At one of the ports I visited, we saw a line of vehicles parked right beside the vessel. We were told that these were the dockworkers' vehicles parked there for convenience. At the time, we were concerned that the vehicles could be hiding places for smuggled drugs. Now we must consider the possibility that a car bomb or a "dirty nuclear weapon" could be hidden in those vehicles.

Many ports do not have ID cards for personnel. I observed all sorts of people milling around at dockside. There was no way to tell who should be there and who should not. The Commission found that, at one port, pedestrians could

freely walk through purported access control points without being questioned. We do not want to contemplate a group of terrorists taking over a cruise ship, but it is a possibility.

Training of security personnel also is a problem. Many seaports use private security personnel who lack crime prevention and enforcement training.

The Commission recommended developing regulations to create a secure area where passengers board and disembark vessels. We also recommended proceeding with an INS project to manage risk with respect to both passengers and crew. We recommended creating shared dockside inspection facilities so that all relevant agencies have ready access to conduct inspections. The Commission called for the establishment of minimum guidelines for physical security, such as fences, lights, gates, restrictions on vehicle access, restrictions on carrying firearms, the establishment of a credentialing process, considering criminal background checks for those with access to sensitive areas of the port, and development of a private security officer certification program. S. 1214 moves in the direction of these recommendations, but it does so through voluntary security guidance. The Committee should consider making some of these requirements mandatory.

Third, we need better information about cargo transitting the ports. On the import side, information is often vague and import entries may be filed 5 days after arrival. On the export side, information tends to be very general (with descriptions like general merchandise) and is required 10 days after export. One of the concerns with providing earlier and more detailed information is that it

would allow specific cargo to be targeted for theft by those with access to the information. This concern needs to be addressed.

Fourth, we need better technology at the seaports. Better technology is needed for a whole variety of applications, which include: x-raying containers, using computer systems to target cargo associated with high terrorist risks; collecting data on crimes at seaports; and providing real-time information for tracking high-risk cargo and personnel.

In sum, the Commission said: A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property and business, affect the operations of harbors and the transportation infrastructure, including bridges, railroads and highways, and cause extensive environmental damage. We need to take action now to reduce the risk of future catastrophes. Thank you for inviting me to testify on this important subject.

ROB QUARTEL

CHAIRMAN AND CEO, FREIGHTDESK TECHNOLOGIES

AND FORMER MEMBER, US FEDERAL MARITIME COMMISSION

TESTIMONY BEFORE

THE

GOVERNMENT AFFAIRS COMMITTEE

OF THE

UNITED STATES SENATE

DECEMBER 6, 2001

I would like to thank the members of this Committee for their invitation today. I will be pleased to submit more detailed testimony after the hearing in order to amplify some of my remarks. In advance of that I have submitted some written material in addition to a power point presentation given several weeks ago to the Container Cooperative Group at the US Department of Transportation, and which I have shared with members of the US Coast Guard, Customs, and other public and private officials. The presentation details a concept which I have called "Pushing the Borders Back" and which I would like to describe briefly to you today, as well as some of the consequences of it.

I have been asked to talk to several issues relating to port security, the working of the international freight system and the role of the ports in it, and to add some thoughts on how the private sector and the federal government might beneficially interact to maintain the security of the system.

Let me start with my central premise, which is that the action isn't at the port. If a terrorist device gets to a port in the United States, it's almost too late. 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.

In my mind, interdiction of terrorist activities really begins at the beginning – with the shipper and his customer, at both the physical and transactional start of an order. I suggest to this committee that it consider the notion of pushing the physical border back Electronically – to create a virtual border, if you will, that resides overseas not just in, but prior to the thousands of ports of embarkation, all the way back to the factory loading dock.

First, for all of the reasons described in testimony earlier today, and despite the low probabilities associated with any given ocean, air, or land-delivered international container, I believe that we should treat every container destined to enter or pass through the United States 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.

The logical consequence of that thought is, second, that no container should be loaded on a ship or train or plane destined for the United States without having been profiled, screened, and if necessary physically inspected. We can't allow a suspect container to reach a port for inspection there, because the port is a potential target. We can't allow it on the ship because ships – some 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 a container while on the high seas. These boxes are from 20-48 feet in length, 8 wide and high, and can weigh 20 tons or more and be stacked 9 deep in the hold of a container ship. It's simply too late to inspect a container on arrival in a US port.

If it's too late to inspect them on arrival here, then can we inspect all of them somewhere else, for example in overseas ports? If we did, could we control it? And is physical inspection any better than other methods? Before I get to that and some alternatives, let me talk to several other issues.

This first slide illustrates a key point: International trade is a tremendously complex business. A typical trade, in fact, may 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 and some 200 different data elements. Each container is valued, on average at $60,000 or more, and most carry cargoes for multiple owners. Some 6 million entered the US in the year 2000, 17,000 a day. There are literally millions of people and hundreds of thousands of companies worldwide 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.

The port seems important, and is, because 95 percent of all international trade arrives in the US by ship – some 20 percent of the US economy The typical ship entering our waters will carry from 4000-6000 TEU's (the equivalent of a 20x8x8 foot container), twice the size the industry thought was viable just ten years ago. An 8000 ship is already on the drawing board, and some experts expect ships of nearly twice that size in the not too distant future. A large vessel may generate over 40,000 documents on docking in a port, and the value of the cargo one of these ships may carry may reach half a billion dollars. The overall value of the trade with the United States is in the neighborhood of $700 plus billion just in cargo value. .

If we were to add a physical inspection to one of the very large ships carrying 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 over 250 man-days to the time it took to offload the ship. Today, a ship is loaded and unloaded in a day or a day and a half, depending on the port. Estimates vary as to the number of ships which dock here each day from 300-500, but we do know that 17,000 containers arrived here last year, and that the volume of this trade is expected to double – double – before the year 2010. Assuming the same labor requirement, that's nearly 3 additional man-years per day, some 1000 over the course of a year.

But the ship isn't the whole story and that really is my third point. A lot of the discussion here is about protecting the port, which is natural given the legislation before the committee. But the port, frankly, is the least of the problems. 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. But in terms of the system of intermodal trade – shipping, moving goods around the world in international trade – the port is just one – not even the most important – piece of the puzzle. It should be considered the point of last – not first – resort in our war on terrorism.

Just as a note, I will be talking a lot about shippers, carriers, and others today. For those of you who aren't logisticians, the shipper is the owner or producer of the cargo in motion. Transportation providers – ships, trains, planes, and trucks – are carriers. Middlemen include forwarders which have historically prepared the documentation, handled the money and arranged for the transport of cargoes overseas, and which today more often than not handle both sides of the transaction; customs brokers, who handle the inbound documentation, storage, and other activities, and consolidators and other middlemen who broker cargo capacity, sometimes act as carriers, and who are now often integrated into the manufacturing process very much as assemblers of finished goods.

As I said in the first slide, international trade is a complicated business. Every trade has a seller and a buyer. Every trade requires a manufacturing event, more often today multiple events and assembly. Every trade requires a land movement or multiple movements – from multiple manufacturing points to an assembly point by truck, from a factory to a rail head to a port. Every intercontinental trade requires a ship or a plane and those from Canada and Mexico will likely use a truck. Once landed in a US port, a truck or a train or a combination of both will move the goods to a destination or multiple destinations. And in between there will be Customs duties, checks, assembly and subassembly movements again before an international shipment finally comes to rest. Typically, some form of middlemen – freight forwarders, customs brokers, consolidators and others – will be involved in expediting the flow, handling the paperwork, or reducing the cost of the move by brokering space or transportation to the benefit of the – usually small – shipper. For the record, some 80 percent or more of US businesses outsource some of all of this process to third parties.

Over 50 percent of what moves is shipped by consolidators, although the largest percentage – perhaps 80-85 percent -- of what they move, according to my sources in the industry, is full container loads rather than actually consolidated from smaller orders.

While this hearing is about ports, the issue is really about the entire transportation and manufacturing process. The USCG Commandant, Admiral Loy, has taken the lead in describing a new way if thinking about the problem that he has called "Maritime Domain Awareness." I would take that one step further – as I show in the slide – to suggest really five transportation systems domains around which we can build a response. The first – the one I view as most important from the standpoint of ultimate security -- is that from manufacturer to port and includes the manufacturing facilities themselves, consolidators, packers, inland transport, and a variety of middlemen. It goes back to where, when, and by whom a container was packed, in addition to the question of with what. I suggest to you that it is in and from this step that the data can be – in fact already is – generated that can provide the principal input to the electronic border. This is a domain dominated largely by the foreign shipper, the foreign middleman, the foreign transporter and foreign port, and by foreign governments. **While we certainly, as the worlds largest trading nation, have leverage with foreign governments here, I believe our greatest leverage lies in the trading relationship itself – between the buyer and seller, both private sector parties**.

The second, as the chart shows, is at the port of embarkation – where we have no jurisdictional reach or authority – but where the physical integrity of the cargo, the ship, and the port facilities themselves continue to be important. It is also at this point, not in an American port, that I would argue the principal interdiction effort should occur. Cargoes that are identified as suspicious should be detained here – prior to loading on a ship for transport into or through the United States – rather than in the US port itself.

The third is the voyage of the ship. Ship ownership, crew integrity, physical integrity of the ship itself require an entirely different response – some physical, and some data based profiling of involved parties, not the least of which are the crew themselves and the party they work for.

The fourth domain is at and around the US port – the domain Admiral Loy has so well articulated, and in which the USCG and US Customs are historically most particularly involved.

And, finally, there is the inland movement in the United States. From the standpoint of security, the issue is to whom is a cargo ultimately going, by which route, and by which transportation means: Who will touch it, who will receive it, how will they use it.

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 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 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 numerous articles and products crucial to everyday life in the United States.

So, I have been over the last several weeks both surprised and not surprised to hear various public officials proclaim that security rather than speed would 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 are some 361 ports in the US, a dozen or so major ones, and hundreds of land border points including airports. Ports that are secure but slow will surely be avoided.

So we can't delay the supply chain and I think it unlikely – if only because it is prohibitively expensive – that we can physically inspect every container and the numerous boxes and orders within it, whether in a US port, on board ship, or at the port of origin.

What does that mean in economic terms? Well, first, we're talking not just labor cost but inventory cost. Logistics costs have steadily declined from 25 percent to lower than 15 percent of GDP over the last 20 years. Inventory is the response companies make if they are uncertain about transportation or suppliers. Carrying costs associated with inventory at rest – goods in storage – in 2000 was nearly $400 billion, about a fourth for interest expense, another fourth for actual warehousing expenses, and the rest for taxes, obsolescence, insurance, etc. Good suppliers and transportation make this expense decline, and it's a number that many economists watch to ascertain the overall efficiency of the system. Bob Delaney, one of the more notable logistics gurus, has estimated that just a five percent addition to inventory – 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, 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, while physical inspection at the port of entry is not only unrealistic but in principal too little, too late, there is an approach which is more holistic and which takes advantage of the dynamics of the modern international trade process. **I believe the solution lies in closely aligning the interests of the government in security with those of the private sector in speed and cost to create a new, more rapid and efficient international transportation system that works not only to our own benefit, but to that of our trading partners.**

It is my belief that we can – and should – literally push the border back, back to the point of origin of every cargo that enters or passes through the United States, through the use and creation of electronic data profiling on every cargo and every container in which it is carried. This virtual electronic border is already in place, in a sense, scattered across millions of documents, reported at varying places in the process – some reported to governments, some maintained in the privacy of the buyer-seller transaction.

In simple terms, I suggest that we create a cargo profiling system that activates prior to the loading of a cargo on a ship, which uses existing commercial data, existing governmental data, and which extends capabilities we already have in the arena of drug interdiction to cover this new problem. (I say virtual here because I'm not sure that it has to be a new data base so much as a means of handling data). The components of the system are already partially in place. **There are several currently reported documents and several privately held documents on the commercial side that could be combined with a government run intelligence and national security data to be combed through this kind of process; and which could form the basis for the pre-release I suggest prior to loading on a US-bound vessel.**

Four existing commercial documents already reported in one form or another to the government would 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: (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. One key flaw, as you can see in the third chart, is that most of this data is reported on the high seas or sometimes even after arrival at Customs. Some of it is never reported to the government, and probably never should unless properly "firewalled" from commercial competitors.

The principal regulatory action here would be to require the reporting of this data prior to the loading of a container onto a ship, for a pre-release or even a pre-clearance by a government agency, probably US Customs.

As happens today on the drug enforcement side, government intelligence and law enforcement data could be combined with an intelligent profiling process or algorithm – that would allow the government to "data mine" the combined data base to profile a cargo based on what it was, who generated it, where and how it moved and where it was going, its intended use.

Validation of the data, normalization of the various data transmissions – the parties to a transaction generate data by a wide variety of technologies, some sophisticated (EDI or web-based), some not (faxes, email) – through a trusted parties process not unlike some Customs and the private sector use today would be a crucial part of the process.

As an aside – and I am not an expert in this part of the process, but do deal with it, "data mining" is the technical term for methods that extract useful knowledge from large sets of data. These methods are already used to assess the risks associated with specific containers, vessels, ports, countries, individuals, or other features of interest. No single method of data mining is sufficient to provide maximum performance in either the short-term or long-term future. We would need to consider a multi-pronged, synergistic approach that combines four important aspects of gleaning insight from the available data.

First, our own knowledge of operations and anomalies can be captured in rules and facts, known as a "knowledge base," 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. Specific knowledge may even identify individual containers that may pose a threat. Some of the anomalies you look for beyond the obvious one of a suspect source area might include a cargo incongruent with its origin; a high value cargo moving on a slow mode; document discrepancies; new shippers or consignees; violations of established shipping or commercial patterns; peculiar transshipments or transportation moves that don't make sense, and so on. The documentation included with this testimony points to some specific documents that might help you detect these particular discrepancies.

Second, in addition to relying on available knowledge, statistical patterns can be identified in risky and threatening shipments, and these patterns can be useful in modifying risk assessments. This is similar to the manner in which an individual's age is often used to modify a physician's assessment of patient risk from various forms of cancer.

Third, mathematical models are required to combine knowledge and statistical patterns into meaningful (numerical) assessments of the risk. The models must be responsive to general and specific inquires and must therefore be flexible and sophisticated. It is

unlikely that traditional mathematical modeling will be sufficient in this regard. Instead, methods based on models of human neural systems (such as "artificial neural networks" in which software is written to mimic the functioning of brains) may be particularly suitable.

Finally, the risk assessment programs or regimen must be updated continually in light of new data to detect changes in patterns and discover novelties. Any fixed assessment system will be defeated. Here, a new branch of artificial intelligence, called evolutionary programming, offers the solution as it enables the risk assessment system to actually invent new rules for detecting threats in much the same way that our own immune systems seeks out new germs.

Cargo profiling is only part of the solution. Programs like the trusted shippers program used to screen cargoes carried in the hold of commercial airliners can be expanded to a larger trusted parties effort. Customs has had some success with public-private partnerships called BASC in interdicting drug trafficking, although even here they will tell you that the success rate is probably at no more than 20 percent.

The newly appointed Customs Commissioner, Robert Bonner, is thinking on somewhat the same lines, and last week announced an effort which is right, but again only a part of the solution: "We must reaffirm the importance of knowing your customer and consider the overall airtightness of your supply chain, from factory floor to loading dock to transportation to our border. Every single link in that chain must be made more secure against the terrorist threat." His specific suggestions included increasing security at the plant or loading dock, enhancing security during transport, whether by land or by sea, making advance manifest information on cargo more accurate and timely, and using electronic seals for container shipments. The companies that do this, he said, "...will be given a 'fast lane' through border crossings and through seaports and others ports of entry."

One flaw – a significant one – is that cargo manifests can only tell you what the ocean carrier knows. If inland transportation was arranged by a third party or the shipper, if the cargo was consolidated elsewhere, the manifest won't show it. Nor is the carrier likely to be voluntarily given all of that information as some of it may be considered proprietary. Data on a container that simply passes through a US port on its way to another country might as well be invisible.

The purpose of this "intelligent electronic border" is to identify cargoes that look suspicious. It's a system that I think Customs has the authority to enforce, given Congressional support, and it is a process that could perhaps be embedded into and as an extension of the Automated Customs Enforcement (ACE) system they are currently building – but which is scheduled to take another five years to deliver. The US Coast Guard also has an extensive law enforcement and national security data base effort 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.

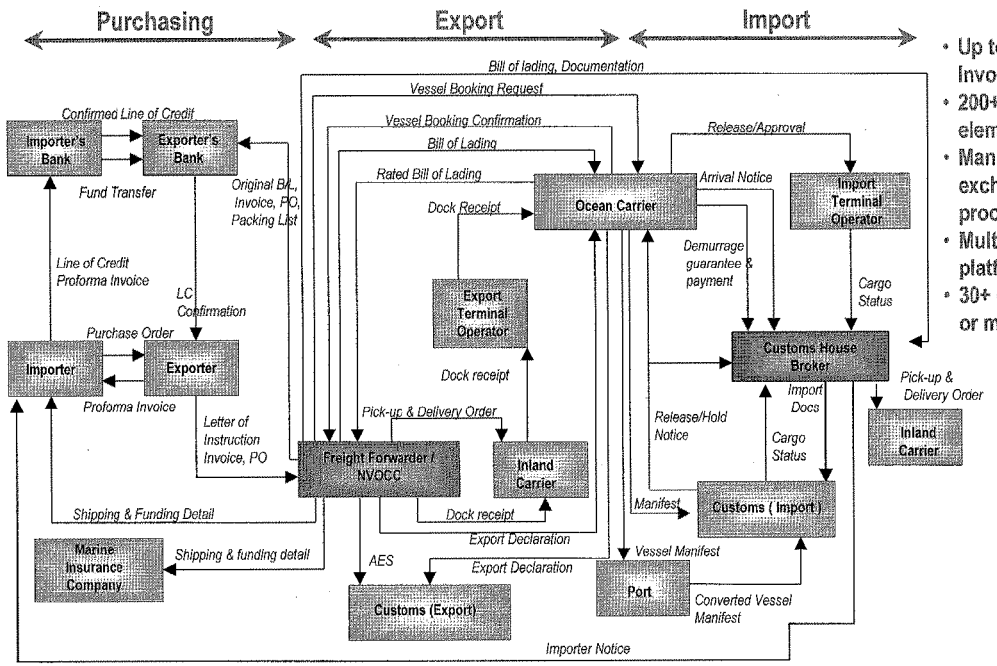
In the hierarchy of responses, this would all be first, intended to intelligently narrow the search. At varying stages across the process we have to layer on passive and physical inspection, physical protection of the ports, protection of the cargo integrity from the basic risks of international transport – spoilage, tampering, theft – the ability to interdict specific cargoes, tracking and visibility solutions that allow us to maintain not only the integrity of the cargo but of the transport system itself. I would be happy to talk to some of these as well.

The critical issue, however, will be to obtain voluntary – not mandatory – commercial compliance with all of the parties in the commercial transaction. Most of the processes covered here are outside the domain of US law enforcement. We can't make foreign suppliers abide by all of these rules, but we can certainly tell their US customers that they may face delays unless they know their sources and can validate cargo and process integrity. We can't 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 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 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 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.

And finally, we really can't tell the US ports that they're the first line of defense. 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.

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

Complex Data Flow for International Shipments

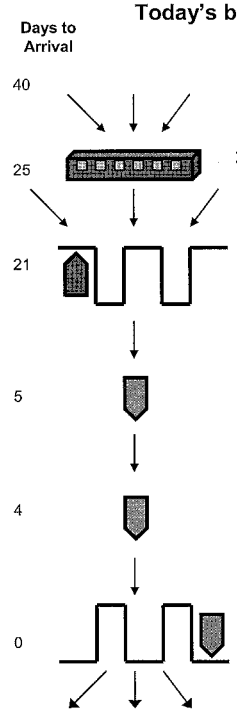


- Up to 20 Involved Parties
- 200+ data elements
- Manual data exchange processes
- Multiple data platforms
- 30+ documents or messages

FreightDesk TECHNOLOGIES

The Information Process Provides an Attraction

Today's border is "fuzzy": data is reported at fluid times and not analyzed for threat



	Process Step	Source of Data
Seller	• Seller and Buyer agree	• Seller generates documents •*Shippers Letter of Instruction* • *Commercial Invoice*
Inland Consolidation Warehouse	• One or more consolidation layers mask goods' origins and involved parties	• Forwarder/consolidator generates documents •*House Bill of Lading*
Foreign Port of Voyage Origin	• Carriers accept containers from multiple sources, with only partial data on contents and origins	• Carrier generates documents •*Master Bill of Lading*
Voyage Underway	• Earliest possible filing of U.S. Customs entry information (ABI)	• Customs broker and/or shipper reporting •*Customs form 7501 and 3461*
Carrier Reporting	• Ship manifest information must be filed by 4 days prior to arrival (AMS)	• Additional carrier reporting •*Shipment Status* •*Vessel Manifest*
First U.S. Destination Port	• U.S. Customs applies physical and commercial border in port zones	• Additional documents may finally be received here •*Surface Bill of Lading*
Buyer		• Buyer generates Purchase •*Purchase Order*

Fluid Time Frame

Border Today

Red documents reported to customs

FreightDesk TECHNOLOGIES

Sample U.S. Import Documents with Major Data Elements

		Import Documentation														
		Used Before Shipment							*Used During Shipment*							
	Data Elements	**Pro-Forma Invoice**	**Packing List**	**Certificate of Origin**	**Shipper's Letter of Instruction**	**Insurance Certificate**	**Inspection Certificate**	**Letter of Credit**	**Commercial Invoice**	**Transmittal Letter**	**Customs Form 7501**	**Bill of Lading**	**Inland Bill of Lading**	**Vessel Manifest**	**Delivery Instruction**	**Customs Form 3461**
1	Invoice Number	■		■	■	■	■	■	■	■	■	■	■	■	■	■
2	Date of Issuance	■		■	■	■	■	■	■	■	■	■	■	■	■	■
3	Shipper's/Exporters name & address	■	■	■	■	■	■	■	■	■		■	■	■	■	
4	Exporter Identification Number (EIN)				■	■	■	■				■	■	■	■	
5	Agent of Exporter				■	■	■	■				■	■	■	■	
6	Intermediate Consignee's name & address	■	■		■	■	■	■		■		■	■	■	■	
7	Ultimate Consignee's name & address	■	■	■	■	■	■	■	■			■	■	■	■	■
8	Quantity	■	■	■	■	■		■	■	■	■		■	■	■	■
9	Unit Price	■	■		■	■		■	■		■		■	■	■	
10	Total Price	■	■		■	■		■	■	■	■		■	■	■	■
11	Net Weight	■	■	■	■	■	■	■	■		■		■	■	■	
12	Gross Weight	■	■	■	■	■	■	■	■		■		■	■	■	
13	Descrition of Merchandise	■	■	■	■				■		■					■
14	Terms of Payment	■							■	■						
15	Incoterms	■			■				■	■						
16	Estimated Shipment Date	■														
17	Currency of Payment	■						■	■	■	■					
18	Time Limit	■						■	■							
19	Miscellanious Charges (FCA, CIF)	■						■	■							
20	Letter of Credit Number							■	■	■						
21	Letter of Credit Date							■	■	■						
22	Import License number								■							
23	Harmonized Commodity number				■				■							■
24	Ocean Carrier Name			■					■		■	■		■		■
25	Ocean Carrier Route								■			■		■		
26	Voyage Number										■	■		■		■
27	Vessel Flag													■		
28	Foreign Port of Export										■			■		■
29	Loading Pier													■		
30	Port of Unloading										■			■		■
31	Method of Transportation															
32	Country of Ultimate Destination				■						■	■				■
33	Bill of Lading Number							■	■							
34	Marks, Nos. & Kinds of Packages		■	■	■											

FreightDesk
TECHNOLOGIES

Sample U.S. Import Documents with Major Data Elements

		Used Before Shipment							Used During Shipment							
	Data Elements	Pro-Forma Invoice	Packing List	Certificate of Origin	Shipper's Letter of Instructions	Insurance Certificate	Inspection Certificate	Letter of Credit	Commercial Invoice	Transmittal Letter	Customs Form 7501	Bill of Lading	Inland Bill of Lading	Vessel Manifest	Delivery Instructions	Customs Form 3461
35	Date of Exportation								■		■			■		
36	Container Number													■		
37	Seal Number													■		
38	Seller's Bank name & address					■		■		■				■		
39	Buyer's Bank name & address					■		■		■	■					■
40	Draft Number									■						
41	Forwarding Date				■	■				■						
42	Purpose of Draft (L/C, Collection, Acceptance)					■				■						
43	Bank Charges							■		■						
44	Protest							■		■						
45	Export Licence Number				■			■								
46	US Port of Arrival										■			■		■
47	Country Which Shipped										■			■		
48	Date of Arrival										■			■		■
49	Country of Origin										■			■		■
50	Point of Origin (City & State)											■				
51	Date of Shipment (Carrier takes control)											■				
52	Delivering Carrier										■	■				■
53	Number of Packages											■				
54	Inland Carrier				■											
55	Shipper's Reference Number				■						■					
56	Date Shipment Send to Forwarder				■											
57	Method of Shipment to Forwarder				■											
58	Insurance				■	■										
59	Shipper Must Check (Prepaid, Collect, COD)				■											
60	Export Control Commodity Number (ECCN)				■											

FreightDesk
TECHNOLOGIES

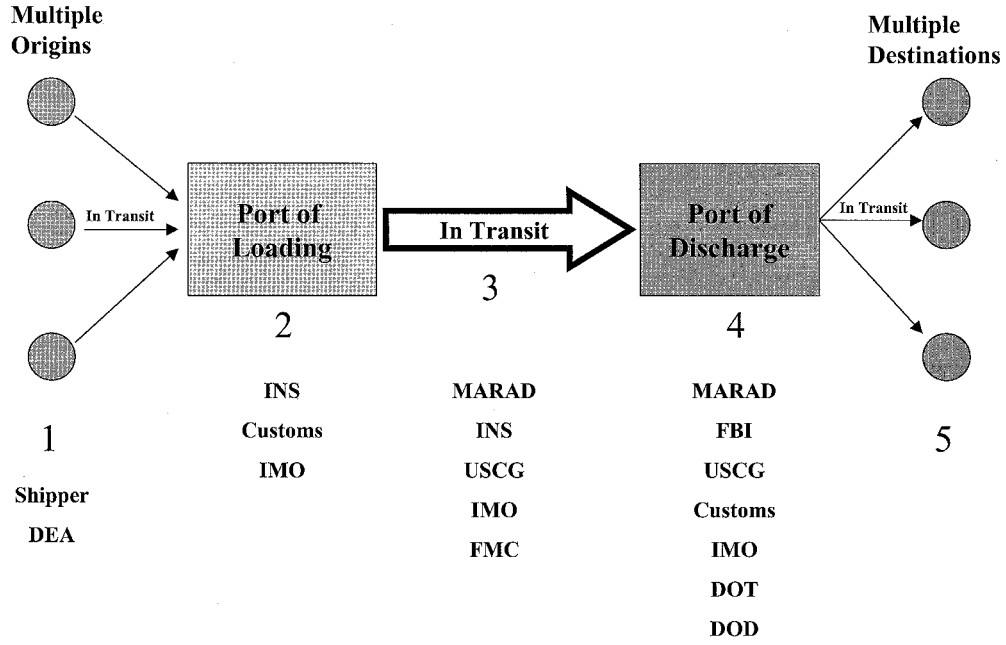
Examples of Anomalies that can be checked using data currently available

Anomaly	Commercial Document	Data element for Anomaly
Cargo Incongruent with Origin	Commercial Invoice, Master Bill of Lading	Routing, Item listing
High value cargo and slow mode	Commercial Invoice, Master Bill of Lading	Item values, routing information
Document discrepancy	Any	Documents do not conform to each other
New Shipper or Consignee	Commercial Invoice, Bill of Lading, Certificate of Origin	Shipper or Consignee Sections
Violation of established shipping or commercial patterns by parties	Any	Any – more in timing/receipt of documents (ex. Once-a-week shipper ships twice in one week)
Suspect source area and transship to small ship	Shippers Letter of Instruction, Bill of Lading	Origin of cargo, route
Point of origin	Shippers Letter of Instruction	Pickup location
Illogical commercial transactions	Commercial Invoice	Comparison of Consignee and Cargo (ex. Furniture company receiving garments)

FreightDesk
TECHNOLOGIES

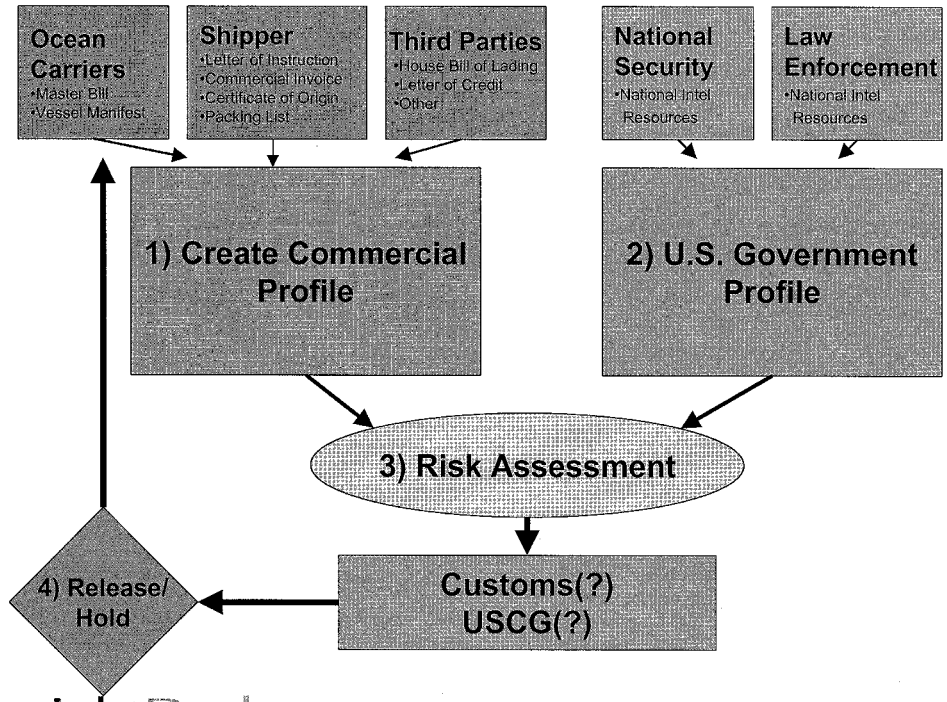
International Freight Movement: Five Domains

Domain Analysis can Suggest a Hierarchy of Responses and Responsibility



FreightDesk TECHNOLOGIES

Profile the Container Prior to Loading



FreightDesk TECHNOLOGIES

STATEMENT OF RICHARD M. LARRABEE
DIRECTOR, PORT COMMERCE DEPARTMENT
THE PORT AUTHORITY OF NY & NJ
ON
ASSESSING THE VULNERABILITY OF U.S. PORTS
BEFORE
THE COMMITTEE ON GOVERNMENTAL AFFAIRS
THE UNITED STATES SENATE
WASHINGTON, DC
DECEMBER 6, 2001

Mr. Chairman, members of the Committee, thank you for the opportunity to testify on the important issue of port security, especially given the events of September 11. I am Rear Admiral Richard M. Larrabee, United States Coast Guard Retired and I am currently Director of Port Commerce at the Port Authority of New York and New Jersey.

The Port of New York and New Jersey is the third largest in the nation and the largest port on the east coast of North America. Last year the port handled over 3 million containers and 560,000 autos. New York/New Jersey handles more petroleum products than any other port in the nation, along with a variety of other bulk and breakbulk commodities. The harbor also supports a wide range of passenger services including cruise ships and growing, as well as increasingly important, commuter ferry services. Ports like New York and New Jersey are key transportation links in global trade; ninety-five percent of US trade comes by ship. The Port of New York and New Jersey serves a region of 18 million people locally and a larger population of 80 to 90 million people within the ten state region surrounding the port. Serving consumer demand for international goods is an essential component of our national economy and ports provide the critical intermodal link for the transfer of those goods from ships to our national landside transportation network.

On September 11, the world witnessed the use of civilian transportation as a weapon to destroy property and take the lives of thousands of innocent people. The

tragic events of that day underscore the critical need to meet America's transportation requirements while ensuring the safety and security of the nation. Much attention has paid to the aviation industry and this is very important given the role of air transportation in our society and economy and the number of citizens that use our aviation system every day. Just as important, however, is our maritime transportation system, which may not move as many people, but is an essential component of our nation's goods movement system and, as a result, is tremendously important to the American economy and national security. Therefore, I thank you, Mr. Chairman, and the Committee for holding this hearing and continuing a national dialogue regarding port and cargo security.

In the immediate aftermath of the attacks on the World Trade Center, the Pentagon and the crash in Pennsylvania, the Port of New York and New Jersey was closed by actions of the US Coast Guard and local law enforcement as a precaution against a potential terrorist threat. This response by Federal, state and local enforcement agencies, along with the support and cooperation of private marine terminal operators and their security teams, was well coordinated and orderly. The port was reopened on the morning of Thursday, September 13 under heightened security measures established by the Coast Guard, Customs, local law enforcement and terminal operators. These measures included at sea boarding of all vessels by joint Coast Guard, Customs and Immigration teams to inspect cargo and crew manifests, tug escort from sea to dock, increased targeting and inspection of cargo containers by joint Federal teams, increased physical security on marine terminals and increased patrols and roadway checkpoints within the port, and restrictions on all foreign crews going ashore.

Under current manning and mission priorities, the Coast Guard and other Federal and state agencies are able to adequately respond in an intensive way to surge port protection, but these organizations can only sustain this level of security for a short period of time. Currently, there are not enough resources in terms of personnel and equipment to maintain that level of security over an extended period within the Port

of New York and New Jersey, let alone the rest of the nation. That is, not without the rest of these agencies core missions being affected. In fact, today there are fewer resources being deployed in the Port of New York and New Jersey than in the days and weeks immediately following the September 11th attacks despite the fact that the threat hasn't changed.

Among the other challenges that we face in addressing the issue of port security are cargo visibility, accountability and responsibility for the contents of containers; the question of "Who is in charge?" in regards to both prevention of and response to a terrorist event; and understanding the threat and vulnerability.

The biggest threat in the maritime industry may not necessarily be a rogue vessel slamming into a bridge, but an intermodal container being used to transport a weapon of mass destruction into the United States. The measures that Customs uses now focus on interdiction but we must focus more on prevention. Given that many major U.S. ports, like New York/New Jersey, are interconnected with national transportation systems and are located near major population centers, interdicting a container laden with a weapon of mass destruction through the inspection of the container here on U. S. soil is too late. Our goal should be to prevent the weapon from ever making it to the United States. The only way to do that is to make maritime security an international issue. Foreign countries must cooperate with us and hold the shipper and port of origin responsible for verifying the contents of a container, similar to what is currently done with the shipment of hazardous materials. Someone must be responsible and held accountable for the contents throughout the entire shipment. From point of origin to point of destination, a chain of custody must be established. Additionally, more detailed cargo information must be provided to U.S. authorities sufficiently in advance of the vessels arrival so that there is a high level of assurance regarding the contents with adequate reaction time if necessary. Admiral Loy addressed the International Maritime Organization (IMO) last week and proposed that a working group be established to look at port security and terrorism, specifically at the issues of cargo visibility and accountability on the part of the port of origin. We

support the Coast Guard's proposal and believe that the IMO is the most appropriate forum to address this issue of international concern.

I know, Mr. Chairman, that you and the members of the Committee are aware that when it comes to preventing or responding to a terrorist incident, the Coast Guard and Customs are only two of several Federal agencies that have a role in port security. In addition, there are state and local agencies that also have port security roles and responsibilities. But one of the fundamental questions still remains, "who's in charge?"

In 1989, in the wake of the Exxon Valdez disaster, we faced a similar question when it came to identifying who was in charge in the event of an oil spill in one of our harbors. Today, we have an answer to that question because the Congress and others took a coordinated approach to developing new laws that laid out clear responsibilities and roles for each of the agencies involved in responding to an oil spill event. This could serve as a model to coordinate the various agency jurisdictions to first prevent and, if necessary, respond to a terrorist attack on our ports. It is an issue we hope that the Office of Homeland Security will address.

Communication is the foundation for coordination among the various agencies responsible for port security. This includes sharing intelligence and threat assessment information among Federal, state and local agencies, as well as certain limited private interests, such as terminal operators, when in those instances the private companies have an explicit responsibility for securing their operations against a potential threat. As a port director, I cannot give you or my superiors a fair assessment today of the adequacy of current security procedures in place because I am not provided with information on the risk analysis conducted to institute these measures.

Mr. Chairman, as you and the Committee members are aware, Senator Hollings has been considering these issues of port security well before the events of September

11. He and Senator Graham are to be commended for their pro-active thinking on these issues. The Senate and others are actively considering the Port and Maritime Security Act of 2001. We look forward to continuing our work with Congress, port operators and private interests to ensure that adequate resources and funding are in place to provide the highest level of security, commensurate with the vulnerability and threat, while also maintaining the safe and efficient movement of commerce and protection of the public.

Our success in providing heightened port security in the wake of the September 11th attacks clearly indicates that no one entity is responsible or capable for providing port security, but rather, it is a shared responsibility among Federal, State and local law enforcement, and private security forces. Thus, any legislation must consider not only those partnerships but also private terminal operators and port authorities. The port industry must have the ability to work together with the local Coast Guard Captain of the Port to develop security guidelines and standards specific to the unique nature and vulnerability of each port area, rather than generic guidelines for all ports.

We commend Senators Hollings and Graham and Transportation Secretary Norman Mineta who, through the Marine Transportation System process, are working to develop a national policy on maritime security.

Providing for national security goes beyond law enforcement procedures and providing adequate resources. Investments in our transportation infrastructure are critical to both our national defense and our economic well-being. Given our heightened awareness of the need for greater security, along with our effort to increase capacity at our ports, we can begin to incorporate security needs into the design and construction of national transportation infrastructure. This could include the application of new technologies that allow us to enhance our security measures while minimizing the impact on the flow of cargo through our transportation systems.

Finally, Mr. Chairman, I want to commend and thank the Coast Guard, the FBI, the U.S. Customs Service, the Immigration and Naturalization Service and a number of other agencies for their tremendous response in the New York/New Jersey region and the unprecedented level of cooperation among Federal agencies and between Federal and local jurisdictions over the past few months. Their efforts are deeply appreciated. Our hope is that the Congress and the Administration will provide these agencies with the tools they need to sustain this level of service to the nation not only in times of crisis, but over the long term.

Thank you, again, for the opportunity to testify. I would be happy to take any questions.

TESTIMONY to the U.S. SENATE, regarding HOMELAND SECURITY
By Deputy Chief C. C. Cook

Good morning to the members of the U.S. Senate, witnesses and others present. I want to give special thanks to Senator Fred Thompson, and in particular his staff, Hannah Sistare, Jason Roehl and Morgan Munchik for inviting me to speak today on behalf of the people of Memphis. I am Deputy Chief Charles S. Cook from the Memphis Police Department here today to talk about the City of Memphis, our preparations for possible terrorist attack, how we have responded to the events of September 11th, and the needs of Memphis in the area of Homeland Security. I am sure our situation is much like those of other cities our size.

Memphis and Shelby County hired an Emergency Management staff, which began to implement and upgrade emergency communication networks and warning devices, such as sirens and the 800 Mhz radio system for interagency communication. The Emergency Management Director began regular meetings and introduced the concept of Emergency Services and designated the various agencies into the 15 service functions. Each agency was given a lead role in at least one function, such as transportation, communications, infrastructure, fire fighting, etc.

The Local Emergency Planning Committee provided its support with numerous resources such as equipment, the expertise of its chemists and technicians and training exercises. The Public Health Department and Hospitals began making their contingency plans and sought grants for various needs. A Tennessee Department of Health grant resulted in the building of a Biological Level "B" Bio-terrorism lab facility under the

Health Department Environmental Services Division which will be capable of testing for Anthrax, Plague, Tularemia and Brucella and provided for the purchase of pharmaceutical stocks, medical supplies and equipment and the development of a medical response plan. This plan includes a biological training program for local health care providers responding to a bio-terrorist incident. This was purchased with funds from a $200,000 Weapons of Mass Destruction grant.

Prior to September 11th, the Memphis Police Department, the local F.B.I., the Memphis/Shelby County Emergency Management Agency, the Memphis and the Shelby County Fire Departments, The City of Bartlett and the City of Germantown Police and Fire Departments began training with Incident Command tabletop exercises. Our focus was on natural disasters, the threat of terrorist attack, school shootings and plane crashes. This multi-agency training developed a team concept in responding to large scale, long duration events. Our departments began seeking further training for various contingencies. In all of the exercises, role players simulated their responses, and as a result of the critiques and follow-ups, determined that additional training, equipment and manpower resources were needed.

Training in Responder Awareness, Operations Awareness, and Incident Command was incorporated into the In-service training programs of the Memphis Police Department. All Memphis officers, and police service technicians are exposed to the training. The Memphis Beale Street Entertainment district began to thrive under downtown renewal projects. Downtown Precinct and Special Operations officers from Tact, Metro Gang, Mounted and Traffic received additional training in crowd control. The use of these officers, in crowd control, became routine and were

often associated with Special Events, such as New Years Eve and other crowd drawing events.

Because of extreme delays on the Memphis to Arkansas bridges across the Mississippi river at I-55 and I-40, caused by relatively simple accidents, a multi-agency " Bridge Mitigation " team was formed in the year 2000. Members of this group came from the police departments of Memphis, Tennessee; and West Memphis, Arkansas; the Sheriffs Departments from Shelby County Tennessee and Crittenden County, Arkansas; the Tennessee Highway Patrol and the Arkansas State Police; the Railroad Police; the Tennessee and the Mississippi Departments of Transportation. Various casualties including marine accidents, terrorist attacks and any subject threatening bridge security became topics of discussion. Decisions regarding multi-agency jurisdiction in removing hazards from the roadway were made. The agencies took joint responsibility for patrolling the bridges.

September 11th

Most police, fire and emergency management agencies, during the first few hours of September 11th, reacted by encircling the government buildings in the downtown area. We deployed our resources to include other targets of opportunity including bridges, water supplies, power and utilities and similar government related services. We received numerous phone calls from businesses, manufacturers, trucking firms, refineries, and other facilities. Each caller was interested in information and what to expect in the way of local terrorist attack. Their questions were addressed through the media in a press conference with public officials including the Memphis Mayor, Shelby county Mayor, the Police Director, the Shelby County Sheriff's Chief Deputy, Fire Director and other emergency service personnel. These officials made an evaluation of the immediate

threat to the city based on information from the F.B.I., and national and local television news. This resulted in an agreement that our response could be reduced. At that time, jointly, in an organized setting, this team of city officials released information to the public. It was timely, informative and reassuring.

This was a unique experience in reality. Elected and appointed public officials guided these many agencies into a team of the various Emergency Services Functions who took the challenge of the day and made joint decisions. The hiring of an Emergency Operations Director and Staff, whose goal was to organize, train and encourage teamwork among Memphis and Shelby Counties Emergency Services, served as a multiplier of the services previously available.

We have experienced a severe blow to our budget as a result of September 11 and our anthrax responses. Sustained actions resulting from hoaxes, threats and actual attacks are devastating to local budgets as you know, draining dollars by eating overtime. There is little that can be held in the hand following unbudgeted responses. Since the events and continuous warnings of future threats, many cities are looking at budget shortfalls.

Following the New York attack, we have experienced the uncertainty and fear of bio-terror. There have been several warnings of additional attacks. As we further assess our ability to deal with attacks of this type, it is necessary to evaluate what is needed in order to defend ourselves against attack, to respond to and reduce the damage and loss of life and to fully recover.

In reviewing the needs of the city, I must mention the Port of Memphis, an integral part of the Memphis economy. Memphis is known as the

America's Distribution Center. I think this notoriety, comes from it's association with Fed-Ex, United Parcel Service and other air carriers. However, the marine port facilities of Memphis metropolitan area is one in only three cities served by 5 class one railroad carriers serving 48 contiguous states, 2 barge fleeting services and a multitude of barge and truck transport services. International shipments come through the Port of New Orleans and are filtered to the other states through Memphis, the worlds' largest cargo airport hub. There are 15 other airlines including U.P.S. conducting operations through this airport. Memphis has a large oil refinery operated by William's Energy with access to McKellar Lake. Memphis has several chemical plants each producing potentially hazardous chemicals. The Tennessee Valley Authority steam plant also has access to McKellar Lake.

The Port of Memphis is the fourth busiest inland port in the country. The port facility has immediate access to interstate 40 and 55 and is located less than 15 minutes from the Memphis International Airport. The Port of Memphis also provides a unique industrial area for the convergence of transportation services located near the Memphis downtown business district.

This transportation hub has been of interest to organized crime due to the large quantity of manufactured goods. The Memphis Police, the Shelby County Sheriff's Office, the local F.B.I., the United States Customs Service, and the National Insurance Crime Bureau was organized through a memorandum of understanding, updated yearly, into the Tennessee, Arkansas, Mississippi Auto Cargo Theft Task Force. This is a multi-agency investigative law enforcement unit targeting organized vehicle theft, including heavy equipment and farm and construction machinery, and associated criminal activity and thefts from interstate cargo shipments.

These are the reasons Memphis is a potential terrorist target.

The following are suggested measures, which should be considered in the interest of preventing terrorist attacks. Attacks which would severely interrupt interstate commerce for years if successful, seriously crippling the nation.

1. Use a multi-agency approach to the investigation of suspected terrorists, and develop the availability of an electronic clearing house for all information gathered nationally and internationally on suspected terrorists.

2. Assign fully armed U.S. Coast Guard personnel to 24 hour operations providing visible patrols on the Mississippi River, Wolf River, McKellar Lake, Tennessee Chute and Frank Pidgeon Industrial Park.

3. Support a national or international truck driver licensing program for drivers entering and exiting the U.S. from Canada and Mexico, and for crossing major infrastructures, bridges, tunnels. Also, support technology capable of identifying drivers and driver history by fingerprint, photos and newer iris scan technology.

4. Support smart card technology for trucks and loads, capable of immediately identifying driver, cargo, origination point, destinations and route plans.

5. Organize a U.S. Coast Guard Inspection Boarding Team to meet and board vessels above and below the Mississippi River bridges to identify operators and crew and to monitor approaches to sensitive

infrastructure such as bridges, industrial complexes and production facilities with river access.

6. Assign U.S. Army or Army Reserve troops to provide 24 hour security/surveillance to the more critical targets, where attacks would cause severe repercussions for America.

7. Provide security gates and barricades limiting access to Presidents Island, refineries and chemical plants from vehicles without the proper identification and authorization.

8. Establish privately owned police agencies like the railroad police and Fed-Ex security police for the protection of businesses which produce or manage critical materials.

9. Establish a Homeland Security Block grant to meet such needs as police and fire overtime, training, communication and rescue equipment and for security measures to protect airports, waterways, utilities, public transit and other public infrastructure.

Thank you once again for inviting me to testify today. I will be happy to work with the committee in the future and at the appropriate time, I will be happy to answer any questions.

Testimony

of

Argent Acosta

President

NTEU Chapter 168

Customs, New Orleans

Before

The Senate Governmental Affairs Committee

December 6, 2001

Chairman Lieberman, Ranking Member Thompson, Members of the Committee, thank you for inviting me here today to talk about Port Security issues. My name is Argent Acosta and I am a Senior Customs Inspector at the Port of New Orleans. I am also the President of Chapter 168 of the National Treasury Employees Union. I have been a Customs Inspector for 30 years.

My job is to ensure that illegal contraband, from knock off designer jeans, to cocaine, to bombs, does not enter the country and that legal goods that enter the country are assessed the correct duties. At seaports, like the Port of New Orleans, the mainstay of the job is boarding incoming vessels, primarily cargo ships, to inspect for illegal goods. It can be a very dangerous and not very glamourous job, but there is a great deal of commitment by front line inspectors to do the best job possible, especially since the events of September 11th.

I would like to share with the Committee a recent example of that commitment. Inspector Thomas Murray, a 31 year veteran of the Customs Service, died tragically during an inspection of the hold of a vessel at the Port of Gramercy in Louisiana on October 30th. He was killed by toxic fumes, as was a member of the vessel's crew and the ship's captain, who followed him into the hold. A second Customs Inspector was overcome by the fumes, but is recovering. Inspector Murray was aware that the vessel he was searching had previously brought illegal drugs into the United States, so he was determined to be as thorough as possible. He didn't know what dangers he would encounter when he went below deck, but he went. Tragically, his commitment to doing his job despite potential danger, cost him his life. His fellow inspectors, especially those of us from Louisiana, will mourn his loss for a long time to come. But we will also remember his bravery and commitment every time we are faced with boarding a suspect vessel or searching a hold that we believe may be dangerous.

Mr. Chairman, you asked in your letter of invitation that I address

several questions regarding port security in my testimony. The first was what is the current adequacy of port security? I'm afraid that I must answer that question by saying that I believe port security is currently not adequate and poses serious potential threats to those not only in the immediate area of the port, but to those who may come in contact with uninspected material that arrives through our ports and moves throughout the country in other modes of transportation.

The Customs Service is currently only capable of inspecting about 2 percent of the 600,000 cargo containers that enter our seaports every day. From my own experience in New Orleans, despite the huge increases in trade since I started with Customs in 1970, the number of Customs Inspectors at the Port of New Orleans has dropped from approximately 103 in 1970 to 29 this year. In addition, since September 11th, Customs Inspectors from around the country have been temporarily reassigned, primarily to the norther border, to cover the gaping holes in security there.

Since I had previously volunteered for Emergency Response Team duties, I was among the first to do a temporary tour of duty in Michigan, at Port Huron, one of the busiest truck crossings in the country. On September 14th, I was given 4 hours to go home and pack and head to Michigan. There was an incredible amount of pressure on inspectors at Port Huron since many "just in time" auto parts headed from Canada to the big three auto makers go through the port. I know my biggest personal concern was not to be the one who let a terrorist into the country and some supervisors seemed to support the view that extreme caution was necessary, but others seemed to be sending the signal that we needed to move things through more quickly because of the need for the auto parts.

I will begin another temporary assignment at Port Huron in January. These temporary reassignments, while currently necessary due to the extreme shortage of personnel, leave the home ports, like my port

of New Orleans, able to inspect even fewer vessels than usual. Also, the more an inspector knows about the particular characteristics of a port, what are the main goods that go through the port, what are the main carriers, destinations, etc. the more effective he or she can be. Obviously, 30 day temporary assignments at different ports does not lend itself to building this kind of experience.

The use of the National Guard at some ports may be temporarily necessary due to the unprecedented threats we are facing, but in many cases, due to their lack of training and experience in the area of cargo and vessel inspection, the National Guard provides the appearance of security rather than any real increase in security. In any case, having military personnel perform these duties is obviously not a long term solution.

In addition to the severe limitations on the ability to do actual inspections, the technology that is supposed to help us do our jobs by providing us with advance information on incoming vessels is outmoded, subject to "brown outs" and often incompatible with the technology of those we need to communicate with. In addition, the advance information about what cargo may be aboard a vessel often is not sent early enough to do any good and even more often is not accurate. Customs has determined that the accuracy rate of vessel cargo information is only 56% accurate.

There are also problems with regard to the physical security of the port. Access to cargo and cruise vessels in many ports is not limited to those with prior approval to be in the area. Virtually anyone can gain access to the areas where vessels unload passengers and cargo. While there are secure areas in the port of New Orleans, access to those areas is overseen by contract security personnel, who, like airport baggage screeners, receive low wages and little training. In fact, in the immediate aftermath of September 11th, while Customs was (it still is) on its highest state of alert, I noted as I passed into the secure area of the

port that there was no one at the security check point, so access to the "secure" area was totally unsecure.

The second question you asked me to address is what problems confront the Customs Service and other federal agencies charged with securing our ports. I believe that the biggest problem is a lack of personnel. As I mentioned earlier, trade has grown exponentially. The number of airports, seaports and border crossings have increased and have seen huge increases in passenger traffic. Funding and personnel levels have not kept up. I believe that funding is also an issue with regard to the use of low wage contract personnel to provide security services to the ports.

Another problem facing Customs in securing our ports is that I believe the balance between rigorous enforcement and facilitation of trade can tip too much toward trade facilitation. In the aftermath of the September 11th attacks there has been a renewed focus on our enforcement role and it has revealed great vulnerabilities. Yes, we need to move trade and people through our ports quickly, but we also need to make sure that we are doing it in a way that protects our security. In order to do both we need more personnel.

Other problems mentioned earlier include lack of adequate technology and timely and accurate manifest information.

The final issue you asked me to address was whether I had any recommendations to address the problems discussed above. The most important recommendation I would make is that Customs needs to be provided with adequate funding. In February of 2000 the Customs Service commissioned a study referred to as the Resource Allocation Model that set optimal staffing levels for Customs at ports throughout the country. That report, which I would like to submit for the record, showed a need for 14,000 additional Customs positions. That was before September 11th. I would hope that Congress would act to provide

these additional positions.

I believe that there is also a need to look at recruitment and retention issues for Customs Inspectors. Their compensation and benefits are less generous than many state and local law enforcement officers and there is a serious concern that experienced Customs Inspectors will leave to become air marshals, due to the more generous compensation package, particularly in the area of retirement. Customs Inspectors should receive the 20 year retirement benefit available to other federal law enforcement personnel if Customs is to remain competitive.

Customs also needs upgraded technology. Congress has provided initial funding for the Automated Commercial Environment or ACE system, which will make remote inspection of cargo more accurate. I must point out, however, that this kind of technology can never take the place of physical inspection.

There is also a need to address physical security issues at our ports by setting up secure areas for incoming cargo and personnel and by ensuring that port security personnel are well trained.

Thank you. I would be happy to answer any questions.

WRITTEN TESTIMONY OF MICHAEL D. LADEN
BEFORE THE
UNITED STATES SENATE
COMMITTEE ON GOVERNMENTAL AFFAIRS
DECEMBER 6, 2001

Mr. Chairman, members of the Committee, good morning. My name is Michael Laden and I am the President of Target Customs Brokers, Inc., a wholly owned subsidiary of Target Corporation. I am also the current Chairman of the American Association of Exporters and Importers (AAEI), and I am an appointee to the Treasury Advisory Committee on the Commercial Operations of the U.S. Customs Service (COAC). I would like to thank you for allowing me the opportunity to express my views on the important matters under consideration today.

First, and most importantly Mr. Chairman, please allow me to make a critical distinction; I am not a self-professed expert on security. I rely on others, including the U.S. Customs Service, for advice and assistance on security matters. What I have to offer the committee today is more than 25 years of practical operational experience on international logistics and customs matters. With that in mind, I'd like to divide my remarks into three separate categories:

- What the trade and Customs have already done to secure international cargo
- What COAC and Customs are currently doing to strengthen security
- What steps the Target Corporation has in place or is considering for the future

From the outset, it is vital for the Committee to keep in mind that the international trade industry is an intricate weave of stakeholders: private and government, foreign and national. Today, the U.S. Customs Service administers more than 400 laws and federal regulations imposed on foreign commerce by more than 40 federal agencies. And, while I would rather be before you today to discuss matters of simplification, the atrocities committed against our nation on September 11th have preempted that discussion. That said, the Committee should know that many of the regulations and laws governing our business are over 200 years old. Given the dynamic nature of modern commerce and the globalization of our economy, many of the regulations we operate under are antiquated, rendering them incompatible with today's modern business practices. Simplification of onerous or outdated regulations designed to expedite the flow of legitimate trade will also result in a significant productivity savings for the U.S. Customs Service, and other regulating agencies. This will allow those agencies to optimize their resources concentrating more on wanton violators and conspirators.

What the Trade and Customs Have Done

I am pleased to report to you that the trade community and the U.S. Customs Service, under the direction of the Treasury Department, are working cooperatively together to improve many of the security features already in place. At the U.S. Customs Trade Symposium held in Washington last week, Customs Commissioner Bonner called upon the trade community to advance the partnership embracing Customs and the trade to a new plateau. Speaking on behalf of Target Corporation, COAC and AAEI, we stand prepared to work side-by-side with Customs in establishing practical, effective and cost efficient to ensure the safekeeping of our supply chain.

The U.S. Customs Service, under the auspices of their Industry Partnership Program (IPP), developed a series of cooperative alliances between Customs, and the trade industry at large. Among these programs are the Carrier, Land Border Carrier and Super Carrier Initiatives. In each of these initiatives, the U.S. Customs Service cooperates with commercial transportation companies to prevent the introduction of contraband into the stream of legitimate commerce. The Customs Service conducts site surveys, if requested, and also provides extensive training on concealment and narcotics detection. To induce their participation, the degree of a carrier's compliance with the agreement may become a mitigating factor in the assessment of penalties if narcotics are found in a conveyance belonging to them. This is a powerful tool, and today more than 3,800 Carrier Initiative Agreements, and 27 Super Carrier Agreements have been signed.

Rounding out the U.S. Customs IPP portfolio is the Business Anti-Smuggling Coalition (BASC). Created under Commissioner Weiss's administration in 1995, BASC is a business-led, Customs-supported, alliance to combat the unscrupulous contamination of legitimate trade. As the Customs Service became more successful in closing the air and sea smuggling corridors, other concealment techniques evolved. With increased frequency the drug cartels targeted otherwise lawful commercial shipments as their preferred conveyance for the movement of their contraband. Innocent carriers and importers were victimized and publicly embarrassed by these acts. BASC is the corporate equivalent of the "SAY NO TO DRUGS CAMPAIGN" so well known to the American public.

In May of this year, the first ever World BASC Conference was convened in Cartegena, Colombia. Customs officials and business leaders from around the world gathered to honor the accomplishments of BASC, and to become signatories to the first worldwide BASC Agreement. Accentuating the significance of this program and their commitment to it, the Acting Commissioner of U.S. Customs was in attendance, as were the Vice President of Colombia and the majority of his cabinet, and the Secretary General of the World Customs Organization (WCO). More than 15 governments leaders and industry executives entered into the Worldwide BASC Agreement, which defines and adopts a specific set of standards for maintaining cargo security. BASC is a win-win partnership; it is not only endorsed by the WCO, but it has gained the support of the International Chamber of Commerce, as well. The effective BASC and Carrier Initiative Programs were launched in response to supply chain incursions confined to a certain geographic region of our world. So, we have an excellent model from which to build. Using these concepts as a prototype, the programs can be retrofitted to become worldwide in scope.

Actions Currently Underway By COAC and the U.S. Customs Service

On November 17th the Treasury Advisory Committee on the Commercial Operations of the U.S. Customs Service (COAC) met for the first time since the events on 9/11. The 20-member COAC is an expert group of appointees representing the trade community. COAC is a compilation of importers, carriers, customhouse brokers, ports and trade attorneys. This group meets quarterly to provide advice to Treasury officials on Customs matters of particular interest to the trade community. During the November meeting, Under Secretary of Enforcement Gurulé briefed COAC members on issues related to supply chain security, and then authorized COAC to form a Technical Advisory Team on Border Security. A plan for organizing the group was presented and approved by the Under Secretary on November 28, 2001, and the first meeting of that group was held yesterday, December 5, 2001, at Customs Headquarters. The outpouring of support has been both heartening and overwhelming. In the last few days I have fielded calls from the Arizona Governor's Office, practically every major trade association, and a number of other major corporations offering their assistance. As you can readily see, the trade has mobilized quickly and we are working on very tight deadlines. Customs Commissioner Bonner has requested a report in his office no later than December 12, 2001, with a view toward submitting all Technical Advisory Team recommendations to the full COAC on January 25, 2002.

In light of the aforementioned complexities of our industry and cognizant of the fact that this is a significant undertaking, the Technical Advisory Team has been separated into three sub-groups, land, marine and air teams. Teams will be further broken down to address sector disparities for example; under the marine category different sub-groups will study containerized cargo versus bulk. Each group will also examine consolidated shipments versus factory-loaded consignments. As a first step, the teams developed a flow chart of the entire process and identified the critical stakeholders involved. A single import shipment will pass through many different hands and many different checkpoints as it travels to our border. Every hand-off obviously creates new vulnerabilities. In the next week, the teams and process owners will examine their respective areas for vulnerabilities and opportunities to fortify security. In part, I believe that some of the answers to our security concerns lie in new or developing technologies, and perhaps in redesigning and streamlining the information flow, but we must also rely on good old-fashioned common sense and American ingenuity. What it will amount to is building some logic into the systems to recognize anomalies.

During a typical year, the U.S. Customs Service processes 10.8 million trucks; 5.3 million cargo containers; 1.9 million railcars; 786,000 commercial aircraft; 140,000 private aircraft; 220,000 vessels; 123,200,000 vehicles; and 479.8 million passengers. Given the technology and resources available today, it is impractical and impossible to search or examine 100% of these conveyances, cargo and passengers. Physical cargo examinations are time consuming and costly. The infrastructure across our land borders is simply not adequate to accommodate the massive quantities. Our airports and marine terminals will become congested with shipments awaiting inspection.

In today's environment, the U.S. Customs Service in addition to selecting cargo or passengers randomly for inspection uses a risk management tool known as "selectivity" to identify high-risk

shipments. A number of ideas are currently being discussed; including improving the data Customs has at its disposal to conduct selectivity analysis and pre-inspection at origin. But from my perspective, sorting out the "known" from the "unknown" shippers is the most expedient way for Customs to refocus its energies on potentially problematic shipments. Last year, the Customs Service processed shipments entered by more than 400,000 importers. However of that number, the top 10,000 importers are responsible for the vast majority of the import volumes. In recent years given the explosive growth in trade and static resources at Customs, they have migrated to an account based management approach for the top tier of importers. Continued expansion of Customs' account based management philosophy is necessary.

Actions Target Has Taken

One of the first tasks I undertook after joining Target in 1998 was establishing a Target BASC Program. Comparatively, Target does not have substantial volumes of traffic from countries that BASC identifies as high risk. This notwithstanding, some of the basic security standards were embraced when creating the compliance questionnaire used by our compliance inspectors. The Target Assets Protection and Import Administration groups coordinate our BASC participation. The Target Brands group who maintains responsibility for Target's Approved for Purchase Program and foreign-based compliance inspectors provides additional support. Target's bottom line is this: we want no more, nor any less than exactly what we've ordered when it comes to an international consignment. Simply stated, we want no contraband of any kind contaminating our shipments.

The centerpiece of the Target BASC Program is training. Working closely with our vendors and service provides located in high-risk countries, we educate them using seminars, written materials and onsite visits to reinforce our expectations. These efforts are further augmented when the factory is designated for an unannounced compliance inspection performed by Target Brands. These rigorous examinations include a review of the premises and available security features. When concerns arise, we work closely with the factory management to rectify matters.

But the process of screening really begins much further upstream, at the beginning of our relationship with a particular vendor. In my view, for an importer, one of the most crucial aspects of security is having reliable knowledge about the suppliers your company is associated with. A few years ago Target launched the Approved for Purchase Program (AFP) for vendors producing owned brand merchandise and certain other product categories. AFP is analogous to making application to become a Target supplier. The vendor is required to complete a comprehensive "application process" by reviewing an AFP Booklet spelling out all of Target's expectations, terms and conditions. Upon receipt of the AFP information, a supplier profile is created and stored for future use. AFP information provided by the factory is then validated during the facility's first compliance inspection. To further advance Target's commitment to the highest ethical and legal standards, we have recently published and are just beginning to distribute a Vendor Conduct Guide that further spells out Target's expectations related to compliance with all laws. Eventually this document will be distributed across our entire vendor base.

While we will wait until the standards that trade and Customs are presently preparing for COAC are complete, going forward I can envision us taking some or all of the following actions:

- Expanding and restructuring the Target BASC Program into an Anti-Contraband Program that is global in scope
- Enhancing our compliance inspections programs to include a more thorough review of security
- Enlisting the support of our Quality Assurance department who also routinely has inspectors in the factories
- Encouraging our carriers to review and improve their security procedures
- Modifying our training materials to include all of the new features in our Anti-Contraband Program[1]
- Heightening security awareness across our entire supply chain

The Target Assets Protection team responds to all breaches of our supply chain integrity through proactive and reactive investigations. This team is a valuable tool in protecting our brand image. Through the use of third party and in-house investigative resources, all threats to our supply chain are thoroughly scrutinized. This team relies not only on internal data, but also has access to various private and public intelligence sources, law enforcement agencies and industry peers to aid them in identifying threats and trends. The team also routinely interacts with the Overseas Security Advisory Council at the State Department.

In summary, as it is with so many other business critical missions, recurrent and consistent communication is imperative to the success of any program. Target frequently offers customized training programs to ensure that new policies or procedures are implemented uniformly. These training initiatives are the backbone of any change to business practices that directly impact our suppliers.

Let me thank you Mr. Chairman for the attention this committee is giving to the security problem, and for giving me an opportunity to appear here today to offer my views. I am sure that I speak for the entire United States international trade community when I say that we are deeply concerned about security, and determined to prevent U.S. international trade from being exploited for inappropriate purposes. We are eager to work with the Congress to accomplish this noble and patriotic goal.

---

[1] The next Target Vendor Import Training program is scheduled to take place in March 2002. Materials for these sessions are currently in production so it will be easy to incorporate new security information into the documentation. We will also be adjusting our schedule to include a security module in these seminars.

PREPARED FOR
THE COMMITTEE ON GOVERNMENTAL AFFAIRS
December 6, 2001

CARGO SECURITY-A PARADIGM SHIFT

W. Gordon Fink
Emerging Technology Markets

EXECUTIVE SUMMARY

Cargo Security is defined as safe, reliable intermodal movement of goods from the shipper to the consignee with no loss due to pilferage, theft or damage. It includes the key carrier assets that move the goods - the containers, trailers, chassis, tractors, vessels, and rail cars. The combination of 1) a significant increase in demand for information on the status of the goods movement process; 2) increased security and safety concerns; 3) the constant pressure to reduce transportation costs; and 4) the speed of cargo movement have created the need for a paradigm shift.

Technology advancements such as global position location systems, improved communications systems (wireless data and the internet), and manifesting and cargo movement software systems are creating a technology based paradigm shift in Cargo Security. The results will be significant as Cargo Security technology applications are developed, tested, the benefits understood and quantified. Multiple sources of these technologies are emerging resulting in reduced implementation costs. Early adopters will benefit from reduced operating costs, improved safety and security, and increased market share. The U. S. Military and regulatory agencies - such as U. S. Customs - will also be major beneficiaries of Cargo Security technology.

THE DEMAND

The constant demand to reduce the cost of goods sold has focused more emphasis on the transportation system. Just-in-time delivery, reduced inventory, and redistribution of products to meet geographical demand are significant factors in the decision process to achieve the optimum blend of transportation, manufacturing, and administrative costs. Customer satisfaction is becoming a more significant factor in the choice of carrier especially when it relates to reliable location and delivery information.

The recent increase in cargo theft and safety are of growing concern to the transportation industry. Thefts, coupled with the potential to use shipments as "weapons of mass destruction", are placing new demands on Cargo Security. While terminal security has improved, there are significant increases in off terminal theft – ranging from

theft by organized criminal organizations that often have "inside" information on the shipments to thefts that are "targets of opportunity". Access to information technology systems, including "corrupt" employees who gain theft targeting information, is increasing. Any time the cargo is stationary, the vulnerability to theft increases. The FBI recently stated that cargo crime is conservatively estimated at $12 billion per year – "the fastest growing crime problem in U. S." The FBI believes that the growth in cargo theft is due to lax penalties, high profit, and low risk of tracing the stolen goods. There is no central repository for cargo theft statistics including common criminal practices. Theft results in an increase in the cost of doing business including increased insurance rates.

In other areas of criminal activity, shipments imported into the U. S. are often used to conceal illegal goods – narcotics, trademark violations, etc. Recent emphasis on the potential to use cargo containers as "weapons of terror" will increase the need for better information and inspection technology. The results are increased costs as well as the potential for delay in cargo delivery.

Terminal operators and carriers work daily to reduce costs. Improved yard and gate systems, remote monitoring systems for reefer and high value cargo, and more efficient use of assets all contribute to reduced operating costs and the speed of transportation services. The chassis has become a key concern of the transportation industry – especially the ability to meet roadability safety requirements. The challenge and debate continues on the responsibility for chassis safety and liability, especially the inspection and reimbursement for repairs responsibilities. Increasing costs, caused by delays at terminal gates and road congestion, are significant factors impacting transportation system costs.

Hazardous cargo movement is also placing increased demands on the carriers - both in the reporting and storage requirements as well as the increased potential for use of these shipments as "weapons of mass destruction". The list of cargo considered to be hazardous is growing as well as the concerns of the public, the regulatory authorities, the carriers, and the terminal and port operators.

THE TECHNOLOGY RESPONSE

Technology is beginning to address the carriers' operational needs to reduce costs and increase safety and security. Some marine terminals are using Radio Frequency Identification (RFID) tags on their chassis, generator sets, and in a few cases containers to reduce on-terminal costs. At the terminal gate, the relationship with container number and the RFID chassis tag is entered into the manifesting system. These systems are improving the efficiency of terminals including a reduction in gate delays. RFID systems eliminate the need for keystroke date entry systems, thus reducing the frequency of human error and increasing operational efficiency.

Rail carriers have installed RFID tags on all their rolling stock and placed readers on their tracks to provide rail car location. Recent innovations in their information technology systems have integrated the container or trailer number with the rail car identification providing location information on the cargo including the estimated arrival and de-ramp times. Customers who know which rail carrier are moving their cargo can access this

data - often using the internet. Marine terminals are also reading the rail car RFID tag as it enters their terminal and using information provided by the rail carrier to immediately access the in-bound container numbers.

Rail and marine terminals are also using optical character recognition systems to read the container, trailer and chassis number. Driver information entered into the software manifesting system becomes part of the increase in terminal efficiency as well as improving Cargo Security – providing a permanent record for Cargo Security and movement information. Terminal operators are also using technology to remotely monitor the condition of reefer units and high value cargo.

A number of the long haul trucking firms initially installed remote monitoring, location, and communication systems in their tractor units to provide information on the performance of the driver, the tractor, and location of their tractor assets with in-transit cargo. Recently, they have invested in similar technology for trailers, permitting them to independently remotely monitor the trailer location and its status – e.g. connected to a tractor, doors open, doors closed, and volumetric load percentage. Newly developed systems permit the remote locking and unlocking of the transportation container. When theft is detected, the doors can be remotely locked and the truck engine disabled.

Cargo Security is already beginning to benefit from technology. Carriers, working with law enforcement authorities, have used these systems to make cargo theft arrests. The maturity of the technology, coupled with a reduction in cost, have contributed to "making the business case" for the technology investment to monitor the status of their assets - the truck and trailer. Increased asset utilization offsets the need to purchase additional equipment. Carriers are meeting the significant increase in customer demands for more information on their cargo location and estimated delivery time.

While these examples are critical to establishing the maturity and cost of Cargo Security technology, many challenges remain to be addressed. One organization that has taken the lead in the United States to advance cargo handling and Cargo Security is the Cargo Handling Cooperative Program (CHCP). The CHCP is a public-private partnership sponsored by the U. S. Department of Transportations' Maritime Administration. CHCP members include ocean and rail carriers, port authorities, terminal operators, trucking companies, asset lessors, and industry associates. The CHCP is actively working on projects to apply technology to the movement of freight, including Cargo Security, in cooperation with the U. S. Department of Defense Transportation Command (US TRANSCOM) and the Center for the Commercial Deployment of Transportation Technologies (CCDoTT).

The container and the chassis represent a unique challenge. There are physical and operational challenges for the chassis. Chassis are often stacked for efficient storage on the terminal. Stacking can damage RFID tags as well as the new remote monitoring system installations. Sometimes chassis are not returned to the carrier or lessor within the agreed time period thus increasing asset operating costs. The approximately 750,000 chassis in the U. S. are an important part of the container transportation system – both on and off the terminal.

Projects are underway to investigate and test technology to remotely monitor the chassis and container location and status. Emerging technology will permit the remote reporting of the safety and status information on the chassis such as tire pressures, brake system status, lights, geographical location, generator set performance, and container Cargo Security – specifically seal integrity. Communicating this information to the carrier will make a significant contribution to improved Cargo Security and improve the utilization of cargo movement assets.

As previously noted, some of this technology is currently operational on trailers. Electronic cargo seals are currently being tested on "in bond" containers transiting the Northwest Corridor into Canada. This technology, whether in the form of disposable or re-useable seals is viewed as a critical part of insuring the security of the cargo shipped in containers. Knowledge of the containers' location as well as the seal integrity are vital pieces of information that can contribute to increased Cargo Security as well as responding to increased demands for the location, safety and delivery time for cargo that is in-route to or that has departed the carrier's terminal. Technology is the response to the long-standing need for off-terminal information.

The long-term technology vision must address improvements in imported container Cargo Security. One concept is to require pre-inspection at terminals and ports that export containers to the U. S. The container would by imaged at the overseas port with non-intrusive technology similar to the Gamma Ray Imaging System currently being used at the land border crossings into the U. S. from Mexico. Customs would pre-screen the image and compare it with a Gamma Ray Image made upon entry into the U. S. Much of the processing could be automated through the application of image change detection software including the special U. S. Customs container examination techniques. While costly, this technology coupled with the electronic container seal integrity could provide major advances in Cargo Security especially the knowledge that the container has been tampered with prior to its entry into the U. S.

Hazardous cargo shipments also present challenges. The technology responses could employ biometric information of the authorized driver combined with the technology previously described for remote monitoring of the location of the tractor, chassis or trailer. Systems could track the location and status of the hazardous cargo to determine if the driver is straying from the "authorized route". This information, in addition to an emergency alarm triggered by a hijacked driver, could immediately provide critical location and hazardous cargo identification information to law enforcement authorities.

The current CHCP program, in partnership with CCDoTT and U. S. TRANSCOM is addressing many of these challenges. The goal is to evaluate existing technology including adapting it to meet Cargo Security, chassis and container monitoring and location requirements. Operational tests utilizing CHCP members' equipment are planned to evaluate available technologies and systems. Requirements not met will be documented for future research projects. The CHCP will describe and quantify the benefits and costs so its members can evaluate their Cargo Security requirements and make their individual business case decisions. The potential benefits are major in meeting the increasing demands of both the private and government sectors.

Port of Portland
Portland International Jetport
Portland Fish Pier Authority
Portland Intermodal Passenger Facility

CITY OF PORTLAND
Department of Transportation

Capt. Jeffrey W. Monroe
Director

Jeff Schultes, AAE
Jetport Manager

Benjamin Snow, MML
Maritime Manager

October 26, 2001

Senator Susan M. Collins
172 Senate Russell Office Building
Washington, D.C.

Dear Senator Collins:

The inherent security weaknesses in our aviation system were brought into sharp focus on September 11th. These weaknesses had been cited on numerous occasions in reports and studies. The rapid passage of S.1447 should begin the process of rebuilding our aviation security system.

The City of Portland supported passage of S.1447 and we support passage of its related bill H.R. 2951. However, we note that Seaport security is not addressed in depth in either bill. In an address to the Marine Transportation System – National Advisory Council on October 18, 2001, Secretary of Transportation Norman Y. Mineta stated that "although much of the media attention has focused on aviation safety, heighten security and awareness will be required from every mode of transportation. None of us can afford to ignore the critical role of our Marine Transportation System and gateway ports in the battle against terrorism…or their potential vulnerabilities."

"In aviation, our airports have a level of coordinated security preplanning that allowed the FAA to respond quickly to the events of September 11th. We need the same kind of planning structure and response capability in our ports. We need a more consistent framework for improved threat assessment and a set of standardized procedures and protocols to follow."

Today, there are agencies and task forces at work examining issues of maritime security. As they report their findings, we will be contacting your office with our comments. At the present time however, our office supports the following:

S.1429 – Airport and Seaport Terrorism Prevention Act, which amends the Merchant Marine Act, 1936, and directs the Secretary of Transportation to provide grants for seaport security infrastructure improvements for the construction, acquisition, or deployment of surveillance equipment and technology at U.S. seaports. Additionally, it establishes a pilot program to track cargo within the United States, including the development and implementation of anti-tampering standards for cargo containers, and

Two Portland Fish Pier, Suite 307 • Portland, Maine 04101 • (207) 773-1613 • FAX 773-0285
E-mail: jwm@ci.portland.me.us

establishes Domestic Port Security Units that can be rapidly deployed to any port threatened with terrorist activity.

We believe that S.1462, The National Emergency Transportation Coordination Act of 2001, which amends Federal transportation law and establishes the Federal Emergency Transportation Administration within the Department of Transportation is vital to national security. This agency would coordinate domestic transportation during a national emergency, provide notice to other U.S. agencies and state and local governments and establish uniform national standards and practices for transportation during a national emergency.

Today, our seaports, like our airports, are in need of trained personnel whose functions would include perimeter patrol, vehicle and employee checkpoints, parking security and passenger identification. Further, security is needed to check and monitor cargoes. We believe that the mission of the National Guard needs to be extended to our seaports.

Specifically, the City of Portland operates two marine terminals which handle both passengers and cargo and require 24/7 security coverage. The port specifically needs a National Guardsman on each shift at each terminal, for a total of six men. The U.S.C.G. has also requested three National Guardsmen per shift to cover the Casco Bay Bridge.

Lastly, our seaports need financial support immediately. Dramatically increased costs and decreased revenues have crippled the budgets of municipalities, states and port authorities throughout the U.S. A portion of the $40 billion appropriated for support services after the events of September 11th, needs to be allotted to seaports.

We must move quickly on the issue of Maritime Security and support our maritime industries. We request that you look at supporting an expansion of funding for the National Guard to cover public seaport facilities. In addition, we request that Governors be given the authority to expand that coverage under the existing presidential order.

Thank you for your consideration,

Sincerely,

Department of Ports and Transportation

Monroe

Captain Jeffrey W. Monroe M.M.
Director

PRESENTATION ON PORT SECURITY CHALLENGES
TO THE NORTH ATLANTIC PORTS ASSOCIATION
BY
CAPT. JEFFREY W. MONROE, DIRECTOR
PORTS AND TRANSPORTATION DEPARTMENT
CITY OF PORTLAND
DECEMBER 7, 2001

Almost ninety days have passed since the terrorist attacks on America. All of us have faced challenges for which we may have not been fully prepared. Our meeting this week offers us an opportunity to evaluate where we are and where we need to be.

Let us make no mistake about it. We are at war and we need to rise to new levels of professionalism in the management of our ports. Vigilance must now be the norm. This is our first challenge.

My office is constantly monitoring intelligence related to transportation issues. We have reviewed numerous reports and briefing documents. Without exception, they predict the following:

- There will continue to be anti-American activity at-home and abroad.
- Terrorists with access to weapons of mass destruction will use them.
- There are over 1,000 people in the U.S. right now with links to various terrorist groups. This is a greater number of human assets based in this country since the days of the cold war.
- There will be increased potential terrorist activities in our ports.

At the Marine Transportation System Research and Development Conference held in mid-November, Edward Badolato of the National Cargo Security Council identified the following transportation security objectives:

- Develop effective reporting systems;
- Strengthen laws and prosecution;
- Improve the understanding of the nature of Port operations;
- Create task forces to identify issues and situations;
- Increase law enforcement expertise;

- Introduce more effective security using the best new technology.

As transportation professionals, we agree, and have offered a six-point action plan to our congressional delegation to address these concerns:

Point One - Federal Coordination of Transportation Systems

- All of us are aware that our local, state and federal agencies were, in many cases, ill prepared for September 11th and that coordination of information and effort was almost non-existent. We believe that the USCG, Customs and INS need to be brought under one coordinating umbrella.

Point Two – The United States Coast Guard

- Expand the mission of the United States Coast Guard and give them the authority and funding they need to do the job. Today, the USCG is fulfilling roles as diverse as drug traffic monitoring and fisheries enforcement as well as the new requirements of homeland security. They do this work with a national force of 35,000, (which I note, is smaller than the New York City Police Department), and antiquated physical assets. Today's new normalcy requires that the Coast Guard be as well equipped and funded as our other defense forces. We support S.1214 introduced by Senator Hollings, but believe that the funding levels in the bill will need to be increased to meet the Coast Guard's expanded role.

Point Three – Planning and Education

- We need adequate preplanning. The port community needs to put our heads together and develop comprehensive operations and security plans based on a common set of standards. I recognize the intrinsic differences between ports, but there is much that is common and we can assist our government agencies with their missions by developing and using these common standards. And in our planning, we need to remember that as we as we go forward; our ports must be agile enough to accommodate both commercial and military freight and personnel. We will need to consult with the United States Transportation Command to address these issues.

- We need to broaden the scope of maritime education programs throughout this country to

include emergency planning and security programs. We need to develop programs to train today's port personnel and tomorrow's transportation leaders.

Point Four – Technology

- We must support the development of new technology that while maximizing throughput and minimizing handling offers a high level of security screening. As this new technology comes on line, we must make sure that smaller ports are able to avail themselves of these breakthroughs through grants and low interest loans. Security should not be a matter of economic competition between ports. We cannot afford any holes in the dike.

Point Five – Shared Intelligence

- Local, State and Federal agencies must develop shared databases to not only address commodity movements but that also track inventories of critical products such as petroleum.

- These same agencies must also share intelligence relating to terrorist activities and threats. It is difficult to maintain high levels of vigilance, when threat alerts are non-specific.

Point Six – Maritime Domain Awareness

- We must encourage all commercial vessels to join the ports in a heightened sense of awareness to unusual activity at-sea and dockside. This is critical as a force multiplier for strained government agencies. We each know best the behavior of our ports on a daily basis and are well positioned to detect changes in patterns.

- We must examine points of origin in measuring our port's vulnerability to attack. We must encourage the development of port security standards worldwide.

Our second challenge is making sure America recognizes the value of its seaports. We need to be sure that the same level of attention is paid to our maritime security issues, as is the new norm for aviation. Since cargo does not vote, legislators are often drawn to aviation as the standard bearer for transportation issues. We must assist them in a change of focus.

It is our responsibility to insure that our lawmakers understand the value of our ports: that over 90% of international trade moves by water and that seaports are as critical to America as airports.

We must be prepared for what lies ahead. There is no doubt that terrorists will continue to focus their attacks on transportation infrastructure. There is little doubt that our ports will be targeted. We must do everything in our power to protect the commercial business of our ports. We must also accept the responsibility to close the door to those who wish to do us harm. These are the new challenges we must work together to meet.

Thank you.

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 – 2002

February 25, 2000

Table of Contents

1. OPTIMAL STAFFING LEVEL OVERVIEW 1

2. OPTIMAL STAFFING LEVEL METHODOLOGY 3

2.1 MODEL ARCHITECTURE 5
2.1.1 Inputs Workbook 5
2.1.2 Rollup Crosswalk Table 5
2.1.3 Performance Measurement Relationship Map 6
2.1.4 Activity Workbooks 6
2.1.5 Regression Workbooks 7
2.1.6 Results Workbook 8
2.2 ASSUMPTIONS FOR OPTIMAL STAFFING LEVELS 8
2.2.1 Workload Growth 9
2.2.2 Border Presence 9
2.2.3 Enforcement Threat 9

Table of Appendices

APPENDIX A – OPTIMAL STAFFING LEVEL DETAIL BY ASSUMPTION TYPE A-1

APPENDIX B – MASTER LOCATIONS LIST B-1

APPENDIX C – PERFORMANCE MEASUREMENT RELATIONSHIP MAP C-1

APPENDIX D – WORKLOAD GROWTH RATE ASSUMPTIONS D-1

APPENDIX E – BORDER PRESENCE ANALYSIS E-1

APPENDIX F – INSPECTOR ENFORCEMENT THREAT ANALYSIS F-1

APPENDIX G – AGENT ENFORCEMENT THREAT ANALYSIS G-1

APPENDIX H – CEO ENFORCEMENT THREAT ANALYSIS H-1

APPENDIX I – MISSION SUPPORT TO CORE POSITION RATIOS I-1

APPENDIX J – OPTIMAL INSPECTOR STAFFING LEVELS BY LOCATION (PRELIMINARY) J-1

APPENDIX K – OPTIMAL AGENT STAFFING LEVELS BY LOCATION (PRELIMINARY) K-1

APPENDIX L – OPTIMAL CEO STAFFING LEVELS BY LOCATION (PRELIMINARY) L-1

APPENDIX M – OPTIMAL IMPORT SPECIALIST STAFFING LEVELS BY LOCATION (PRELIMINARY) M-1

APPENDIX N – OPTIMAL "ALL OTHER" STAFFING LEVELS BY LOCATION (PRELIMINARY) N-1

Table of Figures

Figure 1 – Customs Salaries & Expenses as a Percentage of Other Related Organizations 1
Figure 2 – Fiscal Year 2000 – 2002 Optimal Staffing Level Summary 2
Figure 3 - Customs Occupation By Location Table 4
Figure 4 - RAM Technical Architecture 5
Figure 5 - Activity Analysis Logic 6
Figure 6 - Example Regression Line 7
Figure 7 - Enforcement Threat Calculations 10
Figure 8 - Positions Adjusted by Specific Threats 10
Figure 9 - Optimal Staffing Level Detail – Service-wide A-1
Figure 10 - Optimal Staffing Level Detail – All Other A-2
Figure 11 - Border Presence Analysis E-1
Figure 12 - Border Presence Anlaysis - cont. E-2
Figure 13 - Inspector Enforcement Threat Analysis F-1
Figure 14 - Agent Enforcement Threat Analysis G-1
Figure 15 - CEO Enforcement Threat Analysis H-1
Figure 16 - Mission Support to Core Position Ratios I-1

1. Optimal Staffing Level Overview

In recent years, Customs has seen a decrease in the level of funding, relative to other Federal law enforcement agencies and relative to Treasury, while having significantly higher workloads and threat. This trend is evidenced in the chart shown below.

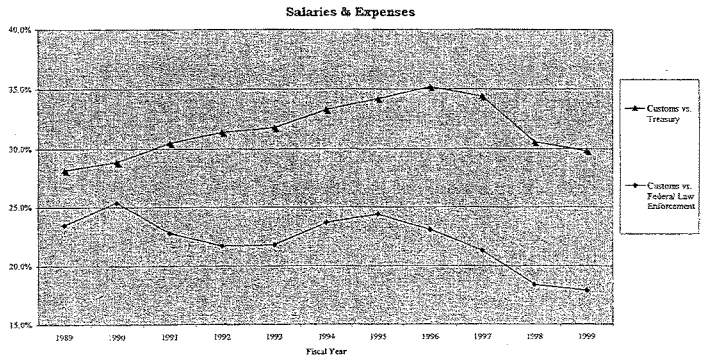


Figure 1 – Customs Salaries & Expenses as a Percentage of Other Related Organizations

Using the Resource Allocation Model (RAM), the U.S. Customs Service reviewed staffing levels and projected the required number of positions to fulfill its mission. Specifically, we found three major challenges to which we needed to respond:

- Workload Growth. The growth of the Customs workload over the past four years has been substantial. Workload drivers for Customs includes such items as number of passengers, number of conveyances and number of containers. Unfortunately, the growth in staff has not kept pace with the growth in the workload across all of Customs activities. For the purposes of this analysis, the RAM was used to predict the required growth in staff driven by the increase in workload. For more detail, see Section 2.2.1.
- Border Presence. Given recent threats identified along our nation's land borders, the U.S Customs Service needs to re-establish a strong presence at all land border ports. To do this, the U.S. Customs Service must increase its staffing at the land border ports to allow 24 hours a day, 7 days a week human coverage of all land border crossings into the United States. Also, to ensure the safety of Inspectors and increase their effectiveness, these crossings will be manned by two Inspectors at all times. For more detail, see Section 2.2.2.

- Enforcement Threat. Over the past four years, workload has grown substantially. However, using number of seizures as a proxy for enforcement threat, the threat has grown at an alarmingly high rate. Consequently, Customs has identified the need for a significant increase in positions to effectively respond to this increasing threat. For more detail, see Section 2.2.3.

The U.S. Customs Service developed scenarios and set assumptions in the RAM to predict the number of positions that would be required to proactively address these three major challenges. The following table is a summary of optimal staffing levels and the required additional number of positions above fiscal year 1998 staffing levels that resulted from that analysis.

	1998 Base	2000	2001	2002
Inspectors	7,677	7,677	7,677	7,677
+ required additional		2,806	4,425	6,481
Total		10,483	12,102	14,158
Agents	2,363	2,363	2,363	2,363
+ required additional		954	1,387	2,041
Total		3,317	3,750	4,404
CEOs	641	641	641	641
+ required additional		275	446	650
Total		916	1,087	1,291
Import Specialists	1,249	1,249	1,249	1,249
+ required additional		128	172	240
Total		1,377	1,421	1,489
All Other	7,498	7,498	7,498	7,498
+ required additional		2,673	3,826	5,364
Total		10,171	11,324	12,862
Service-wide	19,428	19,428	19,428	19,428
+ required additional		6,836	10,256	14,776
Total		26,264	29,684	34,204

Figure 2 – Fiscal Year 2000 – 2002 Optimal Staffing Level Summary

The analysis applied specifically addressed the three major challenges identified for the U.S. Customs Service. For a breakout of the optimal staffing levels, showing required additional positions by assumption type, see Appendix A. The breakout of the optimal staffing levels, showing required additional positions by location, can be found in Appendices J through N. The methodology behind the analysis is detailed in Section 2.

2. Optimal Staffing Level Methodology

The Resource Allocation Model is used as a Customs-wide tool to determine the optimal number of positions by occupation and location. The detailed analysis focuses on core occupations stationed at core locations. Core occupations are defined as those occupations which directly perform one of the four core functions (Passenger Processing, Trade Compliance, Outbound, Enforcement). Core locations are defined as those locations where any core function is directly performed. For a full list of core locations, see the Master Locations list in Appendix B.

The core occupations that are specified for detailed analysis in the model are:

- Inspectors
- Agents
- Import Specialists
- Canine Enforcement Officers (CEOs)
- Entry Specialists
- Regulatory Auditors
- Pilots
- Marine Enforcement Officers (MEOs)

Other occupations were included into a category labeled as Mission Support and a ratio was developed to represent the relationship between the selected occupations and their support requirements.

Customs locations were also divided into core and mission support locations. The RAM will predict the number of staff years for all combinations of location and occupation types:

- Core occupations located at core locations (approximately 68% of Customs fiscal year 1998 staff years)
- Core occupations located at mission support locations (approximately 2% of Customs fiscal year 1998 staff years)
- Mission support occupations located at core locations (approximately 15% of Customs fiscal year 1998 staff years)
- Mission support occupations located at mission support locations (approximately 15% of Customs fiscal year 1998 staff years)

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

However, the main logic of the model is used to predict positions for core occupations at core locations. Below is a table displaying the types of Customs core and mission support locations, the list of occupational groupings, and the intersections of core occupations and core locations.

	CMC	Port	SAC	RAC	Air Branch	Air Unit	Foreign Attaches	STC	Reg. Auditing Division	HQ	Other Mission Support
Inspectors											
Agents											
Import Specialists											
CEOs											
Entry Specialists											
Regulatory Auditors											
Pilots											
MEOs											
Mission Support											

Figure 3 - Customs Occupation By Location Table

The main logic of the RAM predicts staff years for the darkened cells. All other occupation/location combinations are considered Mission Support and predicted using ratios to the core occupation/location combinations.

2.1 Model Architecture

The model is comprised of seven linked Microsoft Excel workbooks. Below is an illustration of the technical architecture of the RAM.

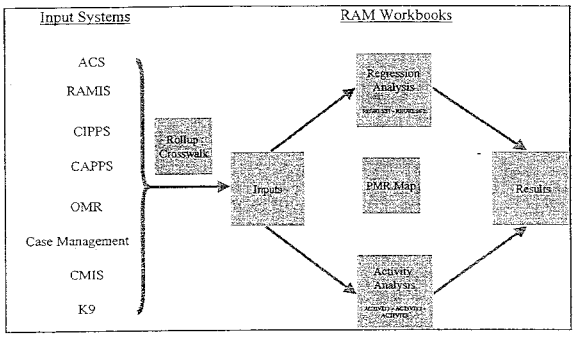


Figure 4 - RAM Technical Architecture

2.1.1 Inputs Workbook

The Inputs workbook is designed to collect and organize the data from the various Customs information systems, including:

- Customs Integrated Personnel/Pay System (CIPPS)
- Operations Management Report Database (OMR)
- Cost Management Information System (CMIS)
- Case Management Information System
- Detector Dog System (K9)
- Regulatory Audit Management Information System (RAMIS)
- Customs Automated Port Profile System (CAPPS)
- Automated Commercial System (ACS)

2.1.2 Rollup Crosswalk Table

The Rollup Crosswalk table is a spreadsheet within the Inputs workbook used to re-format all input data into the Inputs workbook databases. It is used to crosswalk all system codes into

Organization Codes and rollup all levels of location to one, common level. This rollup results in a list of 462 unique locations. See Appendix B for this list.

2.1.3 Performance Measurement Relationship Map

The Performance Measurement Relationship (PMR) Map is the guide that is used to create the logic of the workbooks. The PMR Map (illustrated in Appendix C) details workload drivers, activity time, and results data sources for all of Customs core functions and core occupations in Passenger Processing, Trade Compliance, Outbound, and Enforcement.

2.1.4 Activity Workbooks

The Activity workbooks are designed to calculate the predicted staff years required to accomplish the workload at each of Customs core locations. The staff year is the product of the workload and the activity time per workload, or workload activity time. The workload activity time is the average amount of personnel time that is required to process one workload transaction. For example, for the *Process All Air Primary Passengers* activity, the workload activity time is the average amount of time that is required to process one air passenger at a location.

The logic behind the Activity Analysis workbook is defined in the Performance Measurement Relationship Map (PMR Map). The PMR Map details workload drivers, activity time, and results data sources for all of Customs core functions and core occupations in Passenger Processing, Trade Compliance, Outbound, and Enforcement. The PMR Map is illustrated in Appendix C. Figure 5 is an illustration of the general logic behind the Activity workbooks:

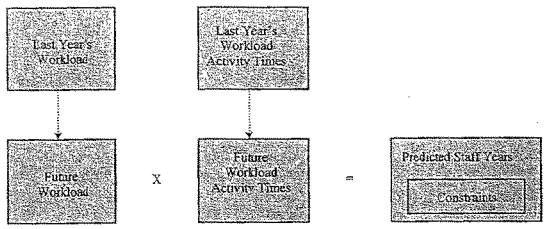


Figure 5 - Activity Analysis Logic

For each occupation performing each specific activity, the Activity workbooks will perform the following calculations:

1. Extract data for last year's workload from the Inputs workbook.
2. Based on growth assumptions that are in the Results workbook, predict new workloads for the future year.
3. Extract last year's average activity time from the Inputs workbook.

4. Select either last year's workload activity time or a user-entered workload activity time, if one is entered. The workload activity time is the average amount of time that it takes to process one workload transaction.
5. Multiply the future workload by the future workload activity time to determine predicted staff years.

2.1.5 Regression Workbooks

The purpose of the regression analysis for the RAM is to provide a check for the predicted staff years determined through the activity analysis. The RAM regression analysis should never be used to predict optimal staffing levels on its own. Regression analysis describes the cause and effect relationship between independent variables (i.e. Number of passengers processed) and a dependent variable (i.e. Number of Customs Inspector staff years). The relationship can be represented by a mathematical formula (e.g., $y = a + bx$) or graphically:

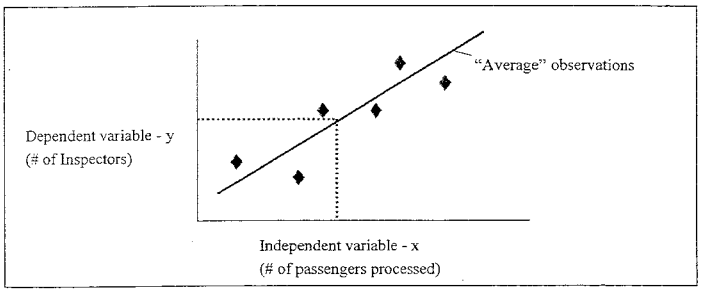


Figure 6 - Example Regression Line

The strength of relationship between the regression line and the data is determined by a statistical factor R^2, ranging from 0 (no relationship) to 1 (perfect relationship). In a perfect world, the variation in the independent variables would explain all the variation in the dependent variable. (i.e. $R^2 = 1$).

Regression models were developed to predict staff years for the following eight core occupations at core locations:

- Inspectors
- Entry Specialists
- Import Specialists
- Canine Enforcement Officers (CEOs)

- Regulatory Auditors
- Agents
- Marine Enforcement Officers (MEOs)
- Pilots

For the FY1998 version of the RAM, predicted staff years for Inspectors, Entry Specialists, Import Specialists and CEOs are estimated for 300 ports. The predicted staff years for Agents, MEOs and Pilots are estimated at various levels. Pilots are measured at the Air Branch/Air Unit levels, which approximates 20 sites. MEOs are measured at the SAC or RAC level, which totals 107 sites. Agents, however, can be at Air branches, Air units, SACs, or RACs, plus they can also be at Foreign Attache sites, bringing their total number of locations to 160. Estimates for Regulatory Auditor staff years are calculated for nine regulatory audit locations, which can then be summed to determine the staff years requirement for Regulatory Auditors at a national level.

2.1.6 Results Workbook

Finally, the Results workbook consolidates the output from the Activity and Regression workbooks and allows the user to investigate "what if" scenarios. Customs may enter numerous assumptions, including the following:

Assumption	Assumption Type
Workload growth rates	Local / Global
Amount of overtime used	Local / Global
All workload activity times (e.g. Primary passenger processing)	Local / Global
Minimum staffing constraints (COBRA & Other)	Local
Congressionally Designated Full-time Positions	Global
Mission Support Assumptions	Local / Global
CMIS Occupation Assumptions	Local
Staff Year Definition (currently 2087 staff-hours)	Global
Staff Day Definition (for CEOs)	Global

Global assumptions can be set once for all locations. Local assumptions can be set separately at each location, overriding global assumptions. It should be noted that the Activity workbooks currently use fiscal year 1998 data as baseline data for the predicted staff years. If Customs leaves all assumptions blank, the number positions predicted by occupation and location will be equal to the actual positions by occupation and location for fiscal year 1998. This flexibility allows Customs to control all of the variables which would influence the allocation of their personnel.

2.2 Assumptions for Optimal Staffing Levels

The following sections describe the three types of assumptions that were set in the RAM to produce the optimal staffing level predictions: workload growth, border presence, and

enforcement threat. Mission Support to core position ratios used to calculate mission support staffing levels are presented in Appendix I.

2.2.1 Workload Growth

To develop the predictions for required additional positions in fiscal years 2000 – 2002, Customs identified global growth rates for most of the workload drivers identified in the PMR Map. These global growth rates were set using straight-line projections based on the past 3-5 years of performance measurement, tempered with some industry data.

For a full list of workload drivers as they relate to Customs activities, see Appendix C – U.S. Customs Service – Performance Measurement Relationship Map. These workload driver growth rates were then applied to fiscal year 1998 baseline data to project required additional positions. For a list of the workload growth rate assumptions applied to fiscal year 2000 – 2002 predictions, see Appendix D.

2.2.2 Border Presence

Given recent threats identified along our nation's land borders, the U.S Customs Service needs to re-establish a strong presence at all land border ports. To do this, the U.S. Customs Service must increase its staffing at the land border ports to allow 24 hours a day, 7 days a week human coverage of all land border crossings into the United States. Also, to ensure the safety of Inspectors and increase their effectiveness, these crossings would be manned by two Inspectors at all times. These requirements result in the following specific assumptions:

- There must be a minimum of 8 Inspector positions to keep a crossing open 24 hours a day, 7 days a week. This breaks down to six 8-hour shifts, plus 25% extra for Training, Leave, Administrative duties, etc.
- There are 93 land border ports included in the analysis. These ports must have at least 8 Inspectors for each crossing for which the port is responsible.

See Appendix E for detailed analysis, showing minimum staffing requirements for each land border port.

2.2.3 Enforcement Threat

Over the past four years, workload has grown substantially. However, using number of seizures as a proxy for enforcement threat, the threat has grown at an alarmingly high rate. Consequently, Customs has identified the need for a significant increase in positions to effectively respond to this increased threat.

Since an exact calculation for total amount of U.S. Customs law violations is not possible, we are forced to use existing data to proxy the enforcement threats posed to the U.S. Customs Service. While the mission of the U.S. Customs Service is very broad and the threats to that mission many, we limited the analysis to three specific types of threat: narcotics, financial (money laundering), and fraud. First, we calculated a proxy for the growth in these three types of threat. Specifically, the threat was calculated as follows:

- ***Narcotics threat.*** An annual increase of 21.9% in the seizures of narcotics between fiscal year 1996 and fiscal year 1999 were used as a proxy for the ongoing increase in narcotics smuggling threat.
- ***Financial threat.*** An annual increase of 14.4% in the seizures of currency between fiscal year 1996 and fiscal year 1999 were used as a proxy for the ongoing increase in financial threat.
- ***Fraud threat.*** An annual increase of 10.5% in the seizures of commercial merchandise between fiscal year 1996 and fiscal year 1999 were used as a proxy for the ongoing increase in fraud threat.

The source data for the calculations is listed below:

Fiscal Year	Total Inspector Positions	Number Of Passengers	Number of Entries	Number Of Containers	Number Of Narcotic Seizures	Number Of Currency Seizures	Number Of Commercial Merchandise Seizures
1996	7,153	445,327,506	13,285,903	9,715,472	23,074	3,008	1,837
1997	7,488	447,186,775	17,810,058	10,164,444	26,771	3,667	2,116
1998	7,677	459,972,488	19,602,074	15,004,608	31,676	4,340	2,367
1999		479,991,352	21,228,253	16,495,572	41,839	4,500	2,481
Annual Growth	3.6%	2.5%	16.9%	19.3%	21.9%	14.4%	10.5%

Figure 7 - Enforcement Threat Calculations

These threat growth rates were then used to calculate the need for additional Inspectors, Agents, and CEOs. Specifically, additional Inspector time would be required in specific activities where narcotic seizures is considered a result. Additional Agent time would be required to address to all three threats, and more. Additional CEO time would be required to address the narcotics and financial threats. To be commensurate with the threat, activity times were increased at the growth rate of the related threat.

Below is a table illustrating the positions that were adjusted according to the specific threats. Appendices F, G, and H provide more detailed analysis as to how the threat rates were applied to the Inspectors, Agents and CEOs, respectively.

	Narcotics	Financial	Fraud	Other
Inspectors	X			
Agents	X	X	X	X
CEOs	X	X		

Figure 8 - Positions Adjusted by Specific Threats

Appendix A – Optimal Staffing Level Detail by Assumption Type

	1998 Base	2000 Workload	2000 Border Presence	2000 Enforcement Threat	2000 Total	2001 Workload	2001 Border Presence	2001 Enforcement Threat	2001 Total	2002 Workload	2002 Border Presence	2002 Enforcement Threat	2002 Total
Inspectors	7,677				7,677				7,677				7,677
+ required additional		722	344	1,740	2,806	998	337	3,090	4,425	1,387	327	4,767	6,481
Total					10,483				12,102				14,158
Agents	2,363				2,363				2,363				2,363
+ required additional				954	954			1,387	1,387			2,041	2,041
Total					3,317				3,750				4,404
CEOs	641				641				641				641
+ required additional		20		255	275	27		419	446	34		616	650
Total					916				1,087				1,291
Import Specialists	1,249				1,249				1,249				1,249
+ required additional		128			128	172			172	240			240
Total					1,377				1,421				1,489
All Other	7,498				7,498				7,498				7,498
+ required additional		974	149	1,549	2,673	1,163	146	2,516	3,826	1,424	142	3,798	5,364
Total					10,171				11,324				12,862
Service-wide	19,428				19,428				19,428				19,428
+ required additional		5,844	493	4,498	6,836	2,360	483	7,412	10,256	3,085	469	11,222	14,776
Total					26,264				29,684				34,204

Figure 9 - Optimal Staffing Level Detail – Service-wide

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

	1998 Base	2000 Workload	2000 Border Presence	2000 Enforce. Threat	2000 Total	2001 Workload	2001 Border Presence	2001 Enforce. Threat	2001 Total	2002 Workload	2002 Border Presence	2002 Enforce. Threat	2002 Total
Entry Specialists	473				473				473				473
+ required additional		49			49	66			66	92			92
Total					522				539				565
Pilots	274				274				274				274
+ required additional		5			5	24			24	44			44
Total					279				298				318
MEOs*	53				53				53				53
+ required additional													
Total					53				53				53
Regulatory Auditors	321				321				321				321
+ required additional		356			356	356			356	356			356
Total					677				677				677
Customs Aides	997				997				997				997
+ required additional		91	34	198	323	175	33	347	507	174	32	533	739
Total					1,320				1,504				1,736
Intelligence Specialists	362				362				362				362
+ required additional				129	129			187	187			276	276
Total					491				549				638
International Trade Specialists	108				108				108				108
+ required additional		11	3	25	39	14	3	42	59	18	3	63	85
Total					147				167				193
Office of Congressional & Public Affairs	27				27				27				27
+ required additional		3	1	6	10	5		10	14	8	1	16	21
Total					37				41				48
Mission Support - Office of Field Operation	1,967				1,967				1,967				1,967
+ required additional		330	67	391	639	248	66	668	1,001	344	64	855	1,463
Total					2,606				2,968				3,430
Office of Finance	468				468				468				468
+ required additional		47	13	109	169	61	12	181	254	80	12	274	366
Total					637				722				834
Office of Human Resource Management	226				226				226				226
+ required additional		23	6	53	82	29	6	87	123	38	6	133	177
Total					308				349				403
Office of Information & Technology	386				386				386				386
+ required additional		39	10	90	139	50	10	160	210	66	10	226	302
Total					525				596				688
Office of Internal Affairs	145				145				145				145
+ required additional		15	4	34	52	19	4	56	79	22	4	85	113
Total					197				224				258
Office of International Affairs	73				73				73				73
+ required additional		2	2	17	26	5	2	28	40	12	2	43	57
Total					99				113				130
Mission Support - Office of Investigations	1,194				1,194				1,194				1,194
+ required additional				424	424			616	616			906	906
Total					1,618				1,810				2,100
Office of Regulations & Rulings	132				132				132				132
+ required additional		13	4	31	48	17	4	51	72	22	3	78	103
Total					180				204				235
Mission Support - Office of Strategic Trade	104				104				104				104
+ required additional		116			116	116			116	116			116
Total					220				220				220
Office of the Chief Counsel	144				144				144				144
+ required additional		13	4	34	52	19	4	56	78	22	4	85	113
Total					196				222				257
Office of the Commissioner	44				44				44				44
+ required additional		4	1	10	15	6		17	24	8	1	26	35
Total					60				68				79
Total - All Other	7,498				7,498				7,498				7,498
+ required additional		974	149	1,549	2,673	1,163	146	2,516	3,826	1,424	142	3,298	4,864
Total					10,171				11,324				12,862

Figure 10 - Optimal Staffing Level Detail – All Other

Appendix B – Master Locations List

RAM Roll-up Code	RAM Roll-up Title
0400000809010110	San Diego Aviation Branch
0400000809010111	Riverside Aviation Unit
0400000809010112	Sacramento Aviation Unit
0400000809010120	Tucson Aviation Branch
0400000809010121	Phoenix Aviation Unit
0400000809010130	Albuqurque Aviation Branch
0400000809010131	El Paso Aviation Unit
0400000809010140	San Angelo Aviation Branch
0400000809010141	San Antonio Unit
0400000809010200	Surv Sup Ctr(Corpus Chris, TX)
0400000809010201	PANAMA AVIATION UNIT
0400000809010310	Jacksonville Aviation Branch
0400000809010311	New York Aviation Unit
0400000809010312	Tampa Aviation Unit
0400000809010320	Houston Aviation Branch
0400000809010321	Kansas City
0400000809010330	New Orleans Aviation Branch
0400000809010331	Pensacola Aviation Branch
0400000809010332	Cincinnati Aviation Branch
0400000809010340	Miami Aviation Branch
0400000809010350	Puerto Rico Aviation Branch
0400000809010351	Gateway - Puerto Rico Air Branch
0400000809010500	Domestic Air Interdictin Coordination Center (DAICC)
0400000809010510	Drug Interdiction Ops Center
0400601600000000	CUST ATTACHE, THE HAGUE NETH
0400601700000000	Senior Customs Rep - Interpol
0400601800000000	Customs Attache - Moscow
0400601900000000	Senior Customs Rep - Hong Kong,BCC
0400602100000000	Customs Attache - London, Eng
0400602200000000	Customs Attache - Pretoria, South Africa
0400602500000000	Customs Attache - Mexico City, Mex
0400602800000000	Customs Attache - Ottawa, Canada
0400603200000000	Customs Attache - Paris, France
0400603400000000	Customs Attache - Rome, Italy
0400603500000000	Customs Attache - Panama City
0400603600000000	CUSTOMS ADVISOR-PANAMA CITY
0400603700000000	Customs Attache - Tokyo, Japan
0400603800000000	Customs Attache - Bonn, Germany

0400603900000000	Customs Attache - Seoul, Korea
0400604000000000	Customs Attache - Bangkok, Thailand
0400604100000000	Customs Attache - Vienna, Austria
0400604300000000	CUSTOMS REP-MILAN, ITALY
0400604400000000	Customs Attache - Singapore
0400604500000000	CUSTOMS REP-MERIDA, MEXICO
0400604600000000	Customs Rep - Monterrey, Mexico
0400604700000000	Customs Rep - Tijuana, Mexico
0400604800000000	Customs Attache - Montevideo, UR
0400604900000000	Customs Attache - Miami, FL
0400605100000000	Customs Attache - Caracas, Venezuela
0400605200000000	Customs Attache - Beijing, China
0400605300000000	Customs Attache - Bogota, Colombia
0400605400000000	Customs Rep- Frankfurt
0400680000000000	Customs Communications Center
0404000000000000	SAC Boston
0404000001000000	RAC Bangor, ME
0404000002000000	RAC New Haven, CT
0404000003000000	RAC Burlington, VT
0409000000000000	SAC Buffalo, NY
0409000001000000	RAC Rouses Point, NY
0410000000000000	SAC New York, NY
0410000001000000	DSAC JFK International Airport
0410000001010000	RAC Long Island
0410000002000000	DSAC Newark, NJ
0410000003000000	DSAC World Trade Center
0413000000000000	SAC Baltimore
0413000001000000	RAC Philadelphia, PA
0413000002000000	RAC Washington, DC
0417000000000000	SAC Atlanta
0417000001000000	RAC Charleston, SC
0417000002000000	RAC Charlotte, NC
0417000003000000	RAC Savannah, GA
0417000004000000	RAC Greenville, SC
0417000005000000	RAC Norfolk, VA
0417000006000000	RAC Wilmington, NC
0418000000000000	SAC Tampa, FL
0418000001000000	RAC Port Canaveral, FL
0418000002000000	RAC Ft. Myers, FL
0418000003000000	RAC Jacksonville, FL
0418000004000000	RAC Orlando, FL
0418000005000000	RAC Panama City, FL
0418000006000000	RAC Pensacola, FL
0418000007000000	RAC Tallahassee, FL

0418000008000000	RAC Sarasota, FL
0420000000000000	SAC New Orleans
0420000001000000	RAC Lafayette, LA
0420000002000000	RAC Baton Rouge, LA
0420000003000000	RAC Lake Charles
0420000004000000	RAC Shreveport, LA
0420000005000000	RAC Little Rock, AR
0420000006000000	RAC Houma, LA
0420000007000000	RAC Gulfport, MS
0420000008000000	RAC Mobile
0420000009000000	RAC Memphis
0420000010000000	RAC Gulf Shores, AL
0420000011000000	RAC Birmingham, AL
0420000012000000	RAC Nashville, TN
0423000000000000	SAC San Antonio, TX
0423000001000000	RAC Brownsville, TX
0423000002000000	RAC San Angelo/Midland, TX
0423000003000000	RAC Mc Allen, TX
0423000004000000	RAC Laredo, TX
0423000005000000	RAC Falcon Dam,TX
0423000006000000	RAC Eagle Pass, TX
0423000007000000	RAC Del Rio, TX
0424000000000000	SAC El Paso, TX
0424000001000000	RAC Albuquerque, NM
0424000002000000	RAC Deming, NM
0424000003000000	RAC Las Cruces, NM
0424000004000000	RAC Alpine
0425000000000000	SAC San Diego
0425000001000000	RAC Oceanside, CA
0425000002000000	RAC Calexico, CA
0425000003000000	RAC San Ysidro, CA
0426000000000000	SAC Tucson
0426000001000000	RAC Phoenix, AZ
0426000002000000	RAC Douglas, AZ
0426000003000000	RAC Nogalas, AZ
0426000004000000	RAC Sellis, AZ
0426000005000000	RAC Yuma, AZ
0427000000000000	SAC Los Angeles, CA
0427000001000000	RAC Los Angeles Intl Airport
0427000002000000	RAC Riverside, CA
0427000003000000	RAC Orange County, CA
0427000004000000	RAC Oxnard, CA
0427000005000000	RAC Las Vegas, NV
0428000000000000	SAC San Francisco, CA

0428000001000000	RAC San Francisco Intl Airport
0428000002000000	RAC San Jose, CA
0428000003000000	RAC Sacramento, CA
0428000004000000	RAC Honolulu, HI
0428000005000000	RAC Salt Lake City
0429000000000000	SAC Denver
0429000001000000	RAC Portland, OR
0430000000000000	SAC Seattle
0430000001000000	RAC Seattle-Tacoma, WA
0430000002000000	RAC Blaine, WA
0430000003000000	RAC Great Falls, MT
0438000000000000	SAC Detroit
0439000000000000	SAC Chicago
0439000001000000	RAC Minneapolis, MN
0439000002000000	RAC Cleveland, OH
0439000003000000	RAC Cincinnati, OH
0439000004000000	RAC St. Louis, MO
0439000005000000	RAC Kansas City, MO
0439000006000000	RAC Indianapolis, IN
0449000000000000	SAC San Juan, PR
0449000001000000	RAC Fajardo, PR
0449000002000000	RAC Mayaguez, PR
0449000003000000	RAC Ponce, PR
0449000004000000	RAC St. Thomas, VI
0452000000000000	SAC Miami, FL
0452000001000000	RAC Ft. Lauderdale, FL
0452000002000000	RAC Ft. Pierce, FL
0452000003000000	RAC Key Largo, FL
0452000004000000	RAC Key West, FL
0452000005000000	RAC West Palm Beach, FL
0453000000000000	SAC Houston
0453000001000000	RAC Galveston, TX
0453000002000000	RAC Corpus Christi, TX
0453000003000000	RAC Dallas, TX
1304000900010000	Port of St. Albans, VT
1304000902000000	Port of Portland, ME
1304000902010000	Port of Jackman, ME
1304000902020000	Port of Bangor, ME
1304000902030000	Port of Bath, ME
1304000902040000	Port of Bar Harbor, ME
1304000902050000	Port of Rockland, ME
1304000902060000	Port of Portsmouth, NH
1304000903000000	Port of Calais, ME
1304000903010000	Port of Eastport, ME

1304000903020000	Port of Vanceboro, ME
1304000903030000	Port of Jonesport, ME
1304000904000000	Port of Houlton, ME
1304000904010000	Port of Van Buren, ME
1304000904020000	Port of Madawaska, ME
1304000904030000	Port of Fort Kent, ME
1304000905000000	Port of Highgate Springs/Alburg, VT
1304000905010000	Port of Richford, VT
1304000905020000	Port of Burlington, VT
1304000906000000	Port of Derby Line, VT
1304000906010000	Port of Norton-Beecher Falls, VT
1304000907000000	Port of Boston, MA
1304000907010000	Port of Springfield, MA
1304000907020000	Port of Worcester, MA
1304000907030000	Port of Gloucester, MA
1304000907040000	Port of New Bedford, MA
1304000908000000	Port of Hartford, CT
1304000908010000	Port of Bridgeport, CT
1304000908020000	Port of New Haven, CT
1304000909000000	Port of Providence, RI
1304000909010000	Port of Newport, RI
1309000900010000	Port of Albany, NY
1309000902000000	Port of Champlain-Rouses Point, NY
1309000902010000	Port of Trout River/Chateaugay/Ft. Covington
1309000903000000	Port of Ogdensburg, NY
1309000903020000	Port of Cape Vincent, NY
1309000903040000	Port of Clayton, NY
1309000904000000	Port of Buffalo, NY
1309000904040000	Port of Syracuse, NY
1310000901000000	Port of New York-Newark
1310000902000000	Port of JFK Airport
1313000900030000	Port of Chester, PA / Wilmington, DE
1313000900040000	Port of Pittsburgh, PA
1313000900050000	Port of Washington, DC
1313000900060000	Port of Alexandria, VA
1313000902000000	Port of Baltimore, MD
1313000902020000	PORT OF CAMBRIDGE, MD
1313000902030000	PORT OF CRISFIELD MD
1313000903000000	Port of Harrisburg, PA
1313000903010000	Port of Wilkes Barre/Scranton, PA
1313000941000000	Port of Philadelphia, PA
1313000941008200	Atlantic City User Fee Airport
1313000941010000	Port of Lehigh Valley, PA
1317000900010000	Port of Charlotte, NC

1317000900020000	Port of Charleston, SC
1317000900030000	Port of Atlanta, GA
1317000902000000	Port of Norfolk, VA
1317000902010000	Port of Newport News, VA
1317000903000000	Port of Richmond-Petersburg, VA
1317000903010000	Port of Charleston, WV
1317000903020000	Port of Front Royal, VA
1317000904000000	Port of Wilmington, NC
1317000904010000	Port of Reidsville, NC
1317000904020000	Port of Beaufort-Morehead, NC
1317000905000000	Port of Durham, NC
1317000905010000	Port of Winston Salem, NC
1317000907000000	Port of Greenville-Spartanburg, SC
1317000907010000	Port of Georgetown, SC
1317000907020000	Port of Columbia, SC
1317000908000000	Port of Savannah, GA
1317000908010000	Port of Brunswick, GA
1318000902000000	Port of Jacksonville, FL
1318000902010000	Port of Fernandina, FL
1318000902020000	Port of Panama City, FL
1318000902030000	Port of Pensacola, FL
1318000903000000	Port of Orlando, FL
1318000903010000	Port of Port Canaveral, FL
1318000903020000	Sanford Regional Airport
1318000903840000	Daytona Beach Regional Airport
1318000903850000	Melbourne Regional Airport
1318000904000000	Port of Tampa, FL
1318000904010000	Port of St. Petersburg, FL
1318000904020000	Port of Manatee, FL
1318000904810000	Ft. Myers Regional Airport
1318000904830000	Sarasota Bradeton Airport
1320000900010000	Port of Mobile, AL
1320000900020000	Port of Gulfport, MS
1320000900030000	Port of Pascagoula, MS
1320000900040000	Port of Birmingham, AL
1320000900050000	Port of Huntsville, AL
1320000900060000	Port of New Orleans, LA
1320000900070000	Port of Memphis, TN
1320000900080000	Port of Baton Rouge, LA
1320000900090000	Port of Morgan City, LA
1320000900100000	Port of Little Rock, AK
1320000900110000	Port of Gramercy, LA
1320000900120000	Port of Greenville
1320000900130000	Port of Vicksburg, MS

1320000900140000	Port of Lake Charles, LA
1320000900150000	Port of Shreveport-Bosier City, LA
1320000900160000	Port of Nashville, TN
1320000900170000	Port of Chattanooga, TN
1320000900180000	Port of Knoxville, TN
1323000900010000	Port of Brownsville, TX
1323000900020000	Port of Del Rio, TX
1323000900030000	Port of Eagle Pass, TX
1323000900040000	Port of Laredo, TX
1323000900050000	Port of Hidalgo, TX
1323000900060000	Port of Roma, TX
1323000900070000	Port of Rio Grande City, TX
1323000900090000	Port of Progreso, TX
1323000902000000	Port of San Antonio,TX
1323000902010000	Port of Austin, TX
1324000900010000	Port of El Paso, TX
1324000900020000	Port of Presidio, TX
1324000900030000	Port of Fabens, TX
1324000900040000	Port of Columbus, NM
1324000900050000	Port of Albuquerque, NM
1324000900060000	Port of Santa Teresa, NM
1325000900011000	Port of San Ysidro, CA
1325000900012000	Port of Otay Mesa , CA
1325000900020000	Port of Tecate, CA
1325000900030000	Port of Calexico, CA
1325000900040000	Port of Andrade, CA
1326000902000000	Port of Douglas, AZ
1326000902010000	Port of Naco, AZ
1326000903000000	Port of Nogales, AZ
1326000903010000	Port of Sasabe, AZ
1326000904000000	Port of Phoenix, AZ
1326000904010000	Port of Tucson, AZ
1326000905000000	Port of San Luis, AZ
1326000905010000	Port of Lukeville, AZ
1327000901100000	Port of Long Beach, CA
1327000901200000	Port of LAX
1328000902000000	Port of San Francisco, CA
1328000902010000	Port of Eureka, CA
1328000902020000	Port of Fresno, CA
1328000902030000	Port of Reno, NV
1328000902040000	Port of Salt Lake City, UT
1328000902050000	Port of San Jose , CA
1328000903000000	Port of Honolulu, HI
1328000903010000	Port of Hilo, HI

1328000903020000	Port of Kahului, HI
1329000900010000	Port of Denver, CO
1329000900018200	Natrona County International Airport
1329000900018300	Jefferson Country Airport
1329000902000000	Port of Anchorage, AK
1329000902010000	Port of Juneau, AK
1329000902020000	Port of Ketchikan, AK
1329000902030000	Port of Skagway
1329000902040000	Port of Alcan, AK
1329000902050000	Port of Wrangell, AK
1329000902060000	Port of Dalton Cache, AK
1329000902070000	Port of Valdez, AK
1329000902080000	Port of Fairbanks, AK
1329000902090000	Port of Sitka, AK
1329000902270000	Port of Kodiak, AK
1329000903000000	Port of Portland, OR
1329000903010000	Port of Astoria, OR
1329000903020000	Port of Newport, OR
1329000903030000	Port of Coos Bay, OR
1329000903040000	Port of Longview, WA
1329000903050000	Port of Boise, ID
1329000903820000	Rogue Valley-Medford User Fee Airport
1330000902000000	Port of Seattle, WA
1330000902010000	Port of Spokane, WA
1330000902820000	Grant County/Moses Lake User Fee Airport
1330000903000000	Port of Blaine, WA
1330000903010000	Port of Sumas, WA
1330000903020000	Port of Point Roberts, WA
1330000903030000	Port of Lynden, WA
1330000904000000	Port of Tacoma, WA
1330000904010000	Port of Aberdeen, WA
1330000904020000	Port of Bellinghham, WA
1330000904030000	Port of Everett, WA
1330000904040000	Port of Port Angeles, WA
1330000904050000	Port of Port Towsend, WA
1330000904060000	Port of Anacortes, WA
1330000904070000	Port of Friday Harbor, WA
1330000904090000	Port OF NEAH BAY,WA
1330000905000000	Port of Oroville, WA
1330000905020000	Port of Danville, WA
1330000905030000	Port of Ferry, WA
1330000905050000	Port of Laurier, WA
1330000905060000	Port of Frontier, WA
1330000905070000	Port of Metaline Falls, WA

1330000906000000	Port of Duluth, MN
1330000906010000	Port of Ashland, WI
1330000906020000	Port of International Falls/Ranier, MN
1330000906030000	PortPortage, MN
1330000907000000	Port of Great Falls, MT
1330000907010000	Port of Raymond, MT
1330000907020000	Port of Eastport, ID
1330000907030000	Port of Butte, MT
1330000907040000	Port of Turner, MT
1330000907050000	Port of Porthill, ID
1330000907060000	Port of Scobey, MT
1330000907070000	Port of Sweetgrass, MT
1330000907080000	Port of Whitetail, MT
1330000907090000	Port of Piegan, MT
1330000907100000	Port of Opheim, MT
1330000907110000	Port of Rooseville, MT
1330000907120000	Port of Morgan, MT
1330000907130000	Port of Whitlash, MT
1330000907140000	Port of Del Bonita, MT
1330000908000000	Port of Pembina, ND
1330000908020000	Port of Portal, ND
1330000908030000	Port of Neche, ND
1330000908040000	Port of St. John, ND
1330000908050000	Port of Northgate, ND
1330000908060000	Port of Walhalla, ND
1330000908070000	Port of Hannah, ND
1330000908080000	Port of Sarles, ND
1330000908090000	Port of Ambrose, ND
1330000908100000	Port of Antler, ND
1330000908110000	Port of Sherwood, ND
1330000908120000	Port of Hansboro, ND
1330000908130000	Port of Maida, ND
1330000908140000	Port of Fortuna, ND
1330000908150000	Port of Westhope, ND
1330000908160000	Port of Noonan, ND
1330000908170000	Port of Carbury, ND
1330000908180000	Port of Dunseith, ND
1330000908190000	Port of Warroad, MN
1330000908200000	Port of Baudette, MN
1330000908220000	Port of Roseau, MN
1330000908810000	Hector User Fee Airport, Fargo
1338000900010000	Port of Detroit, MI
1338000900020000	Port of Port Huron, MI
1338000900030000	Port of Sault Sainte Marie, MI

1338000902000000	Port of Grand Rapids, MI
1338000902010000	Port of Battle Creek, MI
1338000902020000	Port of Saginaw/Bay City/Flint, MI
1338000902030000	Port of Muskegon, MI
1339000900020000	Port of Kansas City
1339000900030000	Port of Cincinnati, OH/Lawrenceburg, IN
1339000900040000	Port of Columbus, OH
1339000900048200	Rickenbacker Airport
1339000900050000	Port of Dayton, OH
1339000900060000	Port of Toledo/Sandusky, OH
1339000900070000	Port of Louisville, KY
1339000900078400	Blue Grass Airport
1339000900080000	Port of Indianapolis, IN
1339000900088300	Baer Field Airport
1339000902000000	Port of Chicago, IL
1339000902010000	Port of Peoria, IL
1339000902020000	Port of Omaha, NE
1339000902030000	Port of Des Moines, IA
1339000902040000	Port of Davenport/Rock Island/Moline, IL
1339000902050000	Port of Rockford
1339000902810000	Waukegan Regional Airport
1339000902830000	Pal-Waukee Airport
1339000903000000	Port of Milwaukee, WI
1339000903020000	Port of Green Bay, WI
1339000903040000	PORT OF SHEBOYGAN, WI
1339000903050000	Port of Racine, WI
1339000904000000	Port of Cleveland, OH
1339000904010000	Port of Erie, PA
1339000904020000	Port of Owensboro, KY/Evansville, IN
1339000904030000	Port of Ashtabula/Conneaut, OH
1339000905000000	Port of St. Louis, MO
1339000905010000	PORT OF ST. JOSEPH, MO
1339000905020000	Port of Wichita, KA
1339000905030000	Port of Springfield, MO
1339000906000000	Port of Minneapolis, MN
1339000906010000	Port of Sioux Falls, SD
1339000906810000	Rochester User Fee Airport
1339000990010000	Vancouver, Canada Preclearance
1339000990020000	Calgary, Canada Preclearance
1339000990030000	Edmonton, Canada Preclearance
1339000990040000	Montreal, Canada Preclearance
1339000990050000	Toronto, Canada Preclearance
1339000990080000	Winnepeg, Canada Preclearance
1339000990090000	Ottawa, Canada Preclearance

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

1349000902000000	Port of San Juan, PR
1349000902020000	Port of Fajardo, PR
1349000902040000	Port of Huamaco, PR
1349000902050000	Port of Mayaguez, PR
1349000902060000	Port of Ponce, PR
1349000902070000	Port of Jobos, OR
1349000903000000	Port of Charlotte Amalie, VI
1349000903020000	PORT OF CORAL BAY VI
1349000903040000	PORT OF FREDERIKSTED VI
1352000900030000	Port of Port Everglades, FL
1352000900040000	Port of West Palm Beach, FL
1352000901010000	Miami Airport
1352000901020000	Miami Seaport
1352000990010000	Nassau, Bahamas
1352000990020000	Freeport, Bahamas
1352000990030000	Kindley Field, Bermuda
1353000902000000	Port of Corpus Christi, TX
1353000903000000	Port of Dallas/Ft. Worth, TX
1353000903010000	Port of Amarillo, TX
1353000903020000	Port of Lubbock, TX
1353000903040000	Port of Oklahoma City, OK
1353000903050000	Port of Tulsa, OK
1353000903820000	Midland Airport
1353000904000000	Port of Houston, TX
1353000904010000	Port of Port Author, TX
1353000904030000	Port of Freeport, TX
1400000001040000	Regulatory Audit Division
9999999999999999	Mission Support

Appendix C – Performance Measurement Relationship Map

The Performance Measurement Relationship (PMR) Map was created to illustrate the links between performance measurements captured by the U.S. Customs Service. The U.S. Customs Service currently captures performance measurement data in a number of different information systems throughout the organization. This data measures many different aspects of the organization including Activity Time, Workload, and Results. However, the RAM project team needed to integrate specific performance measurements into one comprehensive table in order to predict the number of positions by occupation and location. Consequently, the RAM project team developed the PMR Map with the intention of integrating the performance measurement processes for all occupations and core processes at the U.S. Customs Service. Below is a definition of each column in the PMR Map:

Core Function / Occupation. The PMR Map links specific performance measurement data to each of the four core functions (Passenger Processing, Trade Compliance, Outbound, and Enforcement) and eight core occupations identified for the RAM (Inspectors, Agents, Import Specialists, Entry Specialists, CEOs, Pilots, MEOs, Regulatory Auditors). The PMR Map can be expanded to include as many specific programs and occupations as Customs chooses.

Activities. Each of the occupations in the PMR Map will perform one or more activities by which they can be measured. The PMR Map uses activities identified through the Cost Management Information System (CMIS) or through interviews with Customs staff. Each activity has a specific amount of time associated with it that is obtained from Customs data sources and incorporated into the RAM.

Workload Drivers. Workload Drivers are the quantity of events that occur which define the amount of activities that a given occupation must performed in order to accomplish all the respective tasks. For example, the Workload Driver for Air Passenger Processing is the number of air passengers who enter the port. This number dictates how much work must be performed in order to process all of the passengers.

Results. Results are the realized outputs and outcomes from specific activities. For example, a result from examining non-compliant air passengers is seizing narcotics.

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

Core Process / Occupation	Activities	Workload Drivers	Results
Passenger Processing (Inspectors)	Air Passenger Processing – Process all Primary Passengers	# of Inbound Air Primary Passengers	In Process
	Air Passenger Processing – Examine Compliant Passengers	# of Inbound Air Passengers Secondaried that are Compliant (Linked to *Process all Primary Passenger* result)	
	Air Passenger Processing – Examine Non-Compliant Passengers	# of Inbound Air Passengers Secondaried that are Non-compliant (Linked to *Process all Primary Passenger* result)	
	Air Passenger Processing – Process Private Aircraft	# of Inbound Private Aircraft	
	Air Passenger Processing – Informed Compliance	NO WORKLOAD DRIVER	
	Air Passenger Processing – CET Activities	# of Commercial Aircraft	
	Sea Passenger Processing – Process all Primary Passengers	# of Inbound Sea Primary Passengers	
	Sea Passenger Processing – Examine Compliant Passengers	# of Inbound Sea Passengers Secondaried that are Compliant (Linked to *Process all Primary Passenger* result)	
	Sea Passenger Processing – Examine Non-Compliant Passengers	# of Inbound Sea Passengers Secondaried that are Non-compliant (Linked to *Process all Primary Passenger* result)	
	Sea Passenger Processing – Process Private Vessels	# of Inbound Private Vessels	
	Sea Passenger Processing – Informed Compliance	NO WORKLOAD DRIVER	
	Sea Passenger Processing – CET Activities	# of vessels	

Core Process / Occupation	Activities	Workload Drivers	Results
	Land Passenger Processing – Process all Primary Passengers	# of Inbound Land Primary Passengers	
	Land Passenger Processing – Examine Compliant Passengers	# of Inbound Land Passengers Secondaried that are Compliant (Linked to *Process all Primary Passenger* result)	
	Land Passenger Processing – Examine Non-Compliant Passengers	# of Inbound Land Passengers Secondaried that are Non-compliant (Linked to *Process all Primary Passenger* result)	
	Land Passenger Processing – Informed Compliance	NO WORKLOAD DRIVER	
	Land Passenger Processing – CET Activities	NO WORKLOAD DRIVER	
	Passenger Processing – Military Personnel	NO WORKLOAD DRIVER	
Trade Compliance (Inspectors, Import Specialists, Entry Specialists)	Routine/Administrative Processing of Entries & Declarations	# of Entry Releases + # of Entry Summaries	
	Entrance – Vessels & Barges	# of Inbound Vessel Conveyances	
	Entrance – Trucks	# of Inbound Truck Conveyances	
	Entrance – Railcars	# of Inbound Rail Containers Full	
	Entrance – Aircraft	# of Inbound Commercial Aircraft Conveyances	
	CET in Cargo	# of Inbound containers	
	Merchandise Processing / Document Review (Compliance Measurements)	# of Lines Examined + # of Summaries Reviewed for Compliance Measurement	
	Merchandise Processing / Document Review (Excluding Compliance Measurements)	# of Lines Examined + # of Summaries Reviewed, excluding Compliance Measurement	
	Trade Compliance – Informed Compliance	# of Managed Accounts	
	NAFTA Verification	# of NAFTA Verifications, associated with ports	

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

Core Process / Occupation	Activities	Workload Drivers	Results
	Compliance Assessments	# of Compliance Assessments, associated with ports	
	Other Audits	# of Other Audits, associated with ports	
	All International Mail Processing	# of formal entries + # of informal entries + # of exemptions	
	IDs and Brokers Licenses	# of broker applications	
	Application Processing (Other than Brokers Licenses)	# of bonds	
	Work Performed for Other Government Agencies	# of entry releases	
	Express Consignment / Hub Process	# of formal entries + # of informal entries + # of exemptions	
	Trade Compliance – Enforced Compliance	# of referrals to Enforced Evaluation Team (EET)	
Outbound (Inspectors)	Outreach and Informed Compliance	# of people participating in workshops and outreach visits	
	Passenger Analyze and Target	# of Outbound Passengers	
	Routine verification & processing	# of drawback exams + # of vehicle titles processed + # of State Department licensed shipments	
	Passenger Examination	# of Outbound passengers secondaried	
	Passenger Enforcement	Total # of violations from Outbound passengers	
	Cargo Analyze and Target	# of Outbound Bills of Lading (air/sea) + # SEDs (truck/rail)	
	Cargo Examination	# of Outbound cargo exams	
	Cargo Enforcement	# of Outbound cargo violations	
	All Outbound Express Consign Facilities / Hub Process	# of AWBs + # of letter packs	
Mission Support (Inspectors, Import Specialists, Entry Specialists)	Mission Support	NO WORKLOAD DRIVER	
Passenger Processing, Trade Compliance, Outbound, Mission Support (CEOs)	Canine Passenger & Baggage Processing (Inbound and Outbound)	Total # of passengers	

Core Process / Occupation	Activities	Workload Drivers	Results
	Canine Cargo Processing (Inbound & Outbound)	Total # of containers	
	CEO Other Time	NO WORKLOAD DRIVER	
Trade Compliance (Regulatory Auditors)	NAFTA Verifications	# of NAFTA Verifications	
	Compliance Assessments	# of Compliance Assessments	
	Other Audits	# of Other Audits	
	Indirect Time	NO WORKLOAD DRIVER	
	Other Time	NO WORKLOAD DRIVER	
Enforcement (Agents)	Smuggling (General)	# of General Smuggling Cases by Class (Agents)	
	Smuggling (Narcotics) - Mandatory	# of Narcotics Smuggling Cases – Mandatory (Agents)	
	Smuggling (Narcotics) – Discretionary	# of Narcotics Smuggling Cases – Discretionary, by Class (Agents)	
	Fraud	# of Fraud Cases by Class (Agents)	
	Financial (Money Laundering)	# of Financial Cases by Class (Agents)	
	Strategic	# of Strategic Cases by Class (Agents)	
	Cybersmuggling?	# of Cybersmuggling Cases by Class (Agents)	
	Other Case Types	# of Other Case Types Cases by Class (Agents)	
	Non-case hours	NO WORKLOAD DRIVER	
	Other Time (Agents)	NO WORKLOAD DRIVER	
Enforcement (Pilots)	General Investigation	# of Investigative Cases (Pilots)	
	Air Interdiction	# of Interdiction Cases (Pilots)	
	Non-case hours	NO WORKLOAD DRIVER	
	Other Time (Pilots)	NO WORKLOAD DRIVER	
Enforcement (MEOs)	All cases	# of Cases by Class (MEOs)	
	Non-case hours	NO WORKLOAD DRIVER	
	Other Time (MEOs)	NO WORKLOAD DRIVER	

Appendix D – Workload Growth Rate Assumptions

	Predicted Growth from FY1998 to FY...		
Workload Driver	2000	2001	2002
Number of Inbound Air Primary Passengers	10.82%	16.67%	22.85%
Number of Inbound Sea Primary Passengers	14.93%	23.20%	32.07%
Number of Inbound Land Primary Passengers	5.13%	7.76%	10.45%
Number of Entry Releases	20.81%	24.87%	35.03%
Number of Entry Summaries	20.81%	24.87%	35.03%
Number of Vessels & Barges	4.04%	6.12%	8.24%
Number of Truck Conveyances	14.49%	22.50%	31.08%
Number of Full Rail Containers	44.00%	72.80%	107.36%
Number of Aircraft	6.09%	9.27%	12.55%
Number of Inbound Containers	20.53%	32.60%	46.08%
Number of Lines Examined for Compliance Measurement purposes	20.81%	24.87%	35.03%
Number of Lines Examined not for Compliance Measurement purposes	20.81%	24.87%	35.03%
Number of Summaries Reviewed	20.81%	24.87%	35.03%
Number of Outbound Conveyances	17.65%	27.96%	35.11%
Number of Outbound Passengers	6.19%	9.42%	12.76%
Number of CEO Intensive Vehicle Exams	3.23%	4.88%	6.56%
Number of CEO Vehicle Sweeps	3.23%	4.88%	6.56%
Number of CEO Intensive Truck Exams	14.49%	22.50%	31.08%
Number of CEO Truck Sweeps	14.49%	22.50%	31.08%
Number of CEO Intensive Bus Exams	17.07%	26.67%	37.06%
Number of CEO Bus Sweeps	17.07%	26.67%	37.06%
Number of CEO Railroad Car Exams	44.00%	72.80%	107.36%
Number of CEO Commercial Vessel Exams	4.04%	6.12%	8.24%
Number of CEO Cruise Ship Exams	4.04%	6.12%	8.24%
Number of CEO Private Vessel Exams	4.04%	6.12%	8.24%
Number of CEO Commercial Aircraft Exams	6.09%	9.27%	12.55%
Number of CEO Private Aircraft Exams	5.47%	8.32%	11.25%
Number of CEO Intensive Container Exams	20.53%	32.60%	46.08%
Number of CEO Container Sweeps	20.53%	32.60%	46.08%
Number of CEO Passenger Exams	6.19%	9.42%	12.76%

Appendix E – Border Presence Analysis

Port Name	Number of Inspector Positions Predicted for FY2000	Number of Inspector Positions Predicted for FY2001	Number of Inspector Positions Predicted for FY2002	# of Crossings	Minimum # of Inspectors	Additional FY2000 Inspectors Needed	Additional FY2001 Inspectors Needed	Additional FY2002 Inspectors Needed
Port of Jackman, ME	12.6	13.2	13.9	5	40	27	27	26
Port of Houlton, ME	36.1	37.2	38.7	8	64	28	27	25
Port of Trout River/Chateaugay/Ft. Covington	19.0	19.5	20.1	5	40	21	21	20
Port of Richford, VT	16.1	16.6	17.2	4	32	16	15	15
Port of Beecher Falls, VT	20.7	21.9	23.2	4	32	11	10	9
Port of Scobey, MT	1.0	1.0	1.0	1	8	7	7	7
Port of Turner, MT	1.0	1.0	1.0	1	8	7	7	7
Port of Whitetail, MT	1.0	1.0	1.0	1	8	7	7	7
Port of Ferry, WA	1.1	1.1	1.1	1	8	7	7	7
Port of Fortuna, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Hannah, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Hansboro, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Maida, ND	1.0	1.1	1.1	1	8	7	7	7
Port of Morgan, MT	1.1	1.1	1.1	1	8	7	7	7
Port of Neche, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Noonan, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Northgate, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Opheim, MT	1.1	1.1	1.1	1	8	7	7	7
Port of Sarles, ND	1.1	1.1	1.1	1	8	7	7	7
Port of St. John, ND	1.1	1.1	1.1	1	8	7	7	7
Port of Whitlash, MT	1.1	1.1	1.1	1	8	7	7	7
Port of Madawaska, ME	8.6	8.8	9.2	2	16	7	7	7
Port of Ambrose, ND	1.1	1.1	1.2	1	8	7	7	7
Port of Antler, ND	1.1	1.1	1.2	1	8	7	7	7
Port of Carbury, ND	1.1	1.1	1.2	1	8	7	7	7
Port of Sherwood, ND	1.1	1.1	1.2	1	8	7	7	7
Port of Westhope, ND	1.1	1.1	1.2	1	8	7	7	7
Port of Del Bonita, MT	1.3	1.3	1.3	1	8	7	7	7
Port of Point Roberts, WA	1.3	1.3	1.3	1	8	7	7	7
Port of Fort Kent, ME	8.8	9.1	9.4	2	16	7	7	7
Port of Eastport, ID	8.5	9.0	9.5	2	16	8	7	7
Port of Walhalla, ND	2.2	2.2	2.3	1	8	6	6	6
Port of Metaline Falls, WA	2.8	2.9	3.0	1	8	5	5	5
Port of Danville, WA	3.0	3.0	3.1	1	8	5	5	5
Port of Dalton Cache, AK	3.1	3.2	3.3	1	8	5	5	5
Port of Roseau, MN	3.2	3.2	3.3	1	8	5	5	5
Port of Skagway	3.4	3.5	3.7	1	8	5	5	4
Port of Vanceboro, ME	3.5	3.7	3.9	1	8	5	4	4
Port of Laurier, WA	3.8	3.9	4.0	1	8	4	4	4
Port of Frontier, WA	3.9	4.0	4.2	1	8	4	4	4
Port of Porthill, ID	4.1	4.3	4.4	1	8	4	4	4
Port of Sasabe, AZ	5.2	5.3	5.4	1	8	3	3	3
Port of Piegan, MT	5.3	5.4	5.6	1	8	3	3	2
Part of Great Falls, MT	5.6	5.7	5.9	1	8	2	2	2
Port of Warroad, MN	6.5	6.7	6.9	1	8	2	1	1
Port of Dunseith, ND	6.5	6.8	7.1	1	8	2	1	1
Port of Oroville, WA	14.4	14.9	15.5	2	16	2	1	1

Figure 11 - Border Presence Analysis

U.S. Customs Service
Optimal Staffing Levels
Fiscal Years 2000 - 2002

Port Name	Number of Inspector Positions Predicted for FY2000	Number of Inspector Positions Predicted for FY2001	Number of Inspector Positions Predicted for FY2002	# of Crossings	Minimum # of Inspectors	Additional FY2000 Inspectors Needed	Additional FY2001 Inspectors Needed	Additional FY2002 Inspectors Needed
Port of Baudette, MN	7.6	7.8	8.0	1	8	0	0	-
Port of Ketchikan, AK	7.9	8.1	8.3	1	8	0	-	-
Port of Alcan, AK	8.1	8.3	8.6	1	8	-	-	-
Port of Raymond, MT	8.3	8.6	8.9	1	8	-	-	-
Port of Lukeville, AZ	9.6	9.9	10.2	1	8	-	-	-
Port Of Rooseville, MT	9.4	9.7	10.2	1	8	-	-	-
Port of Van Buren, ME	9.7	10.0	10.5	1	8	-	-	-
Port of Lynden, WA	12.2	12.4	12.7	1	8	-	-	-
Part of Portal, ND	12.1	12.4	12.8	1	8	-	-	-
Port of Grand Portage, MN	12.1	12.5	13.1	1	8	-	-	-
Port of Naco, AZ	15.9	16.3	16.8	1	8	-	-	-
Port of Andrade, CA	16.7	17.1	17.5	1	8	-	-	-
Port of Sweetgrass, MT	17.2	17.7	18.6	1	8	-	-	-
Port of Fabens, TX	18.9	19.4	19.8	2	16	-	-	-
Port of Calais, ME	19.5	20.1	21.1	2	16	-	-	-
Port of Santa Teresa, NM	21.6	22.2	23.0	1	8	-	-	-
Port of Columbus, NM	22.6	23.2	24.0	2	16	-	-	-
Port of Tecate, CA	22.5	23.4	24.6	1	8	-	-	-
Port of Sumas, WA	22.7	23.7	24.8	1	8	-	-	-
Port of International Falls/Ranier, MN	22.4	23.8	25.6	1	8	-	-	-
Port of Rio Grande City, TX	24.0	24.6	25.7	2	16	-	-	-
Port of Sault Sainte Marie, MI	24.4	25.1	26.4	1	8	-	-	-
Port of Presidio, TX	26.3	27.0	27.7	1	8	-	-	-
Port of Progresso, TX	29.5	30.3	31.1	1	8	-	-	-
Port of Derby Line, VT	33.7	34.9	36.4	4	32	-	-	-
Port of Roma, TX	35.0	35.8	36.8	2	16	-	-	-
Port of Highgate Springs/Alburg, VT	35.7	37.1	39.0	4	32	-	-	-
Port of Pembina, ND	36.6	38.4	40.9	4	32	-	-	-
Port of Del Rio, TX	46.5	47.8	49.1	2	16	-	-	-
Port of Douglas, AZ	47.5	48.9	50.2	1	8	-	-	-
Port of Ogdensburg, NY	55.6	57.6	59.6	3	24	-	-	-
Port of San Luis, AZ	58.2	59.8	62.0	1	8	-	-	-
Port of Eagle Pass, TX	65.5	67.4	69.8	1	8	-	-	-
Port of Blaine, WA	76.7	78.7	81.7	2	16	-	-	-
Port of Champlain-Rouses Point, NY	77.1	79.3	82.5	5	40	-	-	-
Port of Port Huron, MI	75.2	79.4	85.3	1	8	-	-	-
Port of Hidalgo, TX	141.6	145.0	149.1	2	16	-	-	-
Port of Nogales, AZ	145.9	150.1	155.9	2	16	-	-	-
Port of Otay Mesa, CA	151.2	157.0	165.8	1	8	-	-	-
Port of Brownsville, TX	166.2	171.8	178.2	4	32	-	-	-
Port of Calexico, CA	185.1	193.0	203.4	2	16	-	-	-
Port of Buffalo, NY	194.4	199.9	209.0	4	32	-	-	-
Port of Detroit, MI	231.4	239.8	252.9	2	16	-	-	-
Port of San Ysidro, CA	256.3	263.6	271.3	1	8	-	-	-
Port of Laredo, TX	281.2	295.8	313.1	3	24	-	-	-
Port of El Paso, TX	342.6	352.9	365.7	4	32	-	-	-
Total	3,373	3,487	3,636	155	1,240	344	337	327

Figure 12 - Border Presence Anlaysis - cont.

·cement Threat Analysis

% Increase in re Staff Years from threat growth	% Increase in Core Staff Year from workload Growth	Predicted Additional Core Staff Years	Ratio of MS to Core Staff Years	Predicted MS Staff Years	Total Predicted Staff Years	Average Overtime Rate	Required Additional Positions
48.7%	12.5%	1,505	0.119	179	1,684	19.6%	1,408
48.7%	14.5%	259	0.119	31	290	19.6%	242
48.7%	0.0%	95	0.119	11	107	19.6%	89
							1,740

% Increase in re Staff Years from threat growth	% Increase in Core Staff Year from workload Growth	Predicted Additional Core Staff Years	Ratio of MS to Core Staff Years	Predicted MS Staff Years	Total Predicted Staff Years	Average Overtime Rate	Required Additional Positions
81.3%	16.4%	2,700	0.119	320	3,021	19.6%	2,527
81.3%	22.9%	442	0.119	53	495	19.6%	414
81.3%	0.0%	159	0.119	19	178	19.6%	149
							3,090

% Increase in re Staff Years from threat growth	% Increase in Core Staff Year from workload Growth	Predicted Additional Core Staff Years	Ratio of MS to Core Staff Years	Predicted MS Staff Years	Total Predicted Staff Years	Average Overtime Rate	Required Additional Positions
121.1%	20.5%	4,185	0.119	497	4,682	19.6%	3,916
121.1%	32.4%	672	0.119	80	752	19.6%	629
121.1%	0.0%	237	0.119	28	265	19.6%	222
							4,767

ated at 92.4% of the total activity time spent on the activities.
n the field that may be working in these activities (7575 Inspectors and 623 CEOs).

- Inspector Enforcement Threat Analysis

Appendix G – Agent Enforcement Threat Analysis

Number of Agents Calculations

	2000	2001	2002
FY1998 Base # of Agents	2,363	2,363	2,363
Growth in Narcotics seizures from FY1998	48.6%	81.1%	120.8%
Growth in Currency seizures from FY1998	30.9%	49.7%	71.3%
Growth in Commercial Merchandise seizures from FY1998	22.1%	34.9%	49.1%
Growth in Other threat from 1998	40.2%	66.0%	96.6%
Number of additional Agents to respond to Narcotics Smuggling Cases	563	939	1,399
Number of additional Agents to respond to Financial Cases	139	223	320
Number of additional Agents to respond to Fraud Cases	63	99	139
Number of additional Agents to respond to Other Cases	190	125	183
Total Number of additional Agents required to address threat	954	1,387	2,041

FY1999 Breakout of Case Hours

Division	Percentage
Smuggling (Narcotics)	49%
Financial	19%
Fraud	12%
Strategic	8%
Other	6%
Smuggling (General)	4%
Child Pornography	2%
	100%

FY1996-FY1999 Annual Growth Rates

Result Measure	
Narcotics seizure	21.9%
Currency seizure	14.4%
Commercial merchandise seizure	10.5%
Other threat	18%

Figure 14 - Agent Enforcement Threat Analysis

***Note:** "Other threat" is calculated as a weighted average of smuggling (narcotics), financial and fraud threats. It is weighted by the percentage of activity time that was spent on each threat during fiscal year 1999.

Appendix H – CEO Enforcement Threat Analysis

Number of CEOs Calculations

	2000	2001	2002
FY1998 Base # of CEOs	641	641	641
Growth in Narcotics seizures from FY1998	48.6%	81.1%	120.8%
Growth in Currency seizures from FY1998	30.9%	49.7%	71.3%
Number of additional CEOs to respond to Narcotics Smuggling	156	260	387
Number of additional CEOs to respond to Currency Smuggling	99	159	228
Total Number of additional CEOs	255	419	616

FY1999 Estimate of CEO Hours

Activity	Percentage
Narcotics Smuggling	50%
Currency Smuggling	50%
	100%

FY1996-FY1999 Annual Growth Rates

Result Measure	
Narcotics seizure	21.9%
Currency seizure	14.4%

Figure 15 - CEO Enforcement Threat Analysis

Appendix I – Mission Support to Core Position Ratios

	Ratio
Customs Aides to Office of Field Operations core positions (Inspectors, CEOs, Import Specialists, Entry Specialists)	0.09900
Intelligence Specialists to Office of Investigations core positions (Agents, Pilots, MEOs)	0.13500
Other Office of Field Operations mission support to Office of Field Operations core positions	0.19600
Other Office of Investigations mission support to Office of Investigations core positions	0.44400
International Trade Specialists to all core positions	0.00855
Office of Congressional & Public Affair positions to all core positions	0.00210
Office of Finance positions to all core positions	0.03697
Office of Human Resource Management positions to all core positions	0.01786
Office of Information & Technology positions to all core positions	0.03050
Office of Internal Affairs positions to all core positions	0.01143
Office of International Affairs positions to all core positions	0.00576
Office of Regulations & Rulings positions to all core positions	0.01044
Office of the Chief Counsel positions to all core positions	0.01140
Office of the Commissioner positions to all core positions	0.00351
Office of Strategic Trade positions in the field to Regulatory Auditor positions	0.09585
Office of Strategic Trade positions at Headquarters to Regulatory Auditor positions	0.23053

Figure 16 - Mission Support to Core Position Ratios

Appendix J – Optimal Inspector Staffing Levels by Location (Preliminary)

Note: When calculated to the location level, the optimal additional Inspectors required for enforcement threat (5,080) aggregate to a different number than when calculated globally (4,767). To remain conservative in its estimates and to remain consistent with the other global calculations, Customs chose the smaller of the two numbers to include in its final staffing request.

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
	Total:	7,677	1,387	326	5,080	14,470
1304000900010000	Port of St. Albans, VT	1	0	-	1	2
1304000902000000	Port of Portland, ME	8	1	-	12	21
1304000902010000	Port of Jackman, ME	11	3	26	4	44
1304000902020000	Port of Bangor, ME	9	1	-	5	14
1304000902030000	Port of Bath, ME	-	-	-	-	-
1304000902040000	Port of Bar Harbor, ME	1	0	-	1	3
1304000902050000	Port of Rockland, ME	-	-	-	-	-
1304000902060000	Port of Portsmouth, NH	2	0	-	1	3
1304000903000000	Port of Calais, ME	18	3	-	7	28
1304000903010000	Port of Eastport, ME	5	1	-	4	10
1304000903020000	Port of Vanceboro, ME	3	1	4	2	10
1304000903030000	Port of Jonesport, ME	-	-	-	-	-
1304000904000000	Port of Houlton, ME	33	5	25	10	74
1304000904010000	Port of Van Buren, ME	9	2	-	6	16
1304000904020000	Port of Madawaska, ME	8	1	7	5	21
1304000904030000	Port of Fort Kent, ME	8	1	7	6	22
1304000905000000	Port of Highgate Springs/Alburg, VT	32	7	-	17	56
1304000905010000	Port of Richford, VT	15	2	15	9	41

Organization Code	Location Title	Inspectors				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1304000905020000	Port of Burlington, VT	4	1	-	2	7
1304000906000000	Port of Derby Line, VT	31	5	-	18	54
1304000906010000	Port of Norton-Beecher Falls, VT	19	5	9	10	42
1304000907000000	Port of Boston, MA	91	24	-	52	168
1304000907010000	Port of Springfield, MA	2	0	-	1	3
1304000907020000	Port of Worcester, MA	2	1	-	0	3
1304000907030000	Port of Gloucester, MA	2	0	-	1	3
1304000907040000	Port of New Bedford, MA	2	0	-	1	3
1304000908000000	Port of Hartford, CT	9	2	-	4	14
1304000908010000	Port of Bridgeport, CT	2	0	-	1	3
1304000908020000	Port of New Haven, CT	2	0	-	0	3
1304000909000000	Port of Providence, RI	4	1	-	1	6
1304000909010000	Port of Newport, RI	1	0	-	0	1
1309000900010000	Port of Albany, NY	6	1	-	3	10
1309000902000000	Port of Champlain-Rouses Point, NY	71	12	-	67	150
1309000902010000	Port of Trout River/Chateaugay/Ft. Covington	18	2	20	13	53
1309000903000000	Port of Ogdensburg, NY	52	8	-	37	97
1309000903020000	Port of Cape Vincent, NY	-	-	-	-	-
1309000903040000	Port of Clayton, NY	-	-	-	-	-
1309000904000000	Port of Buffalo, NY	177	32	-	114	323
1309000904040000	Port of Syracuse, NY	5	1	-	3	8
1310000901000000	Port of New York-Newark	395	84	-	183	662
1310000902000000	Port of JFK Airport	591	96	-	445	1,132
1313000900030000	Port of Chester, PA / Wilmington, DE	8	2	-	4	14
1313000900040000	Port of Pittsburgh, PA	13	3	-	9	25
1313000900050000	Port of Washington, DC	64	10	-	61	135
1313000900060000	Port of Alexandria, VA	3	0	-	2	5

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1313000902000000	Port of Baltimore, MD	56	12	-	21	89
1313000902020000	PORT OF CAMBRIDGE, MD	-	-	-	-	-
1313000902030000	PORT OF CRISFIELD MD	-	-	-	-	-
1313000903000000	Port of Harrisburg, PA	3	1	-	1	5
1313000903010000	Port of Wilkes Barre/Scranton, PA	1	0	-	0	2
1313000941000000	Port of Philadelphia, PA	72	16	-	42	131
1313000941008200	Atlantic City User Fee Airport	1	0	-	1	2
1313000941010000	Port of Lehigh Valley, PA	1	0	-	1	2
1317000900010000	Port of Charlotte, NC	16	2	-	22	40
1317000900020000	Port of Charleston, SC	31	8	-	9	48
1317000900030000	Port of Atlanta, GA	68	10	-	46	125
1317000902000000	Port of Norfolk, VA	21	4	-	4	29
1317000902010000	Port of Newport News, VA	3	1	-	0	4
1317000903000000	Port of Richmond-Petersburg, VA	4	1	-	1	6
1317000903010000	Port of Charleston, WV	1	0	-	1	2
1317000903020000	Port of Front Royal, VA	-	-	-	-	-
1317000904000000	Port of Wilmington, NC	5	1	-	3	8
1317000904010000	Port of Reidsville, NC	-	-	-	-	-
1317000904020000	Port of Beaufort-Morehead, NC	3	0	-	1	5
1317000905000000	Port of Durham, NC	8	2	-	3	14
1317000905010000	Port of Winston Salem, NC	3	1	-	0	4
1317000907000000	Port of Greenville-Spartanburg, SC	5	1	-	2	8
1317000907010000	Port of Georgetown, SC	0	0	-	-	1
1317000907020000	Port of Columbia, SC	2	1	-	0	3
1317000908000000	Port of Savannah, GA	15	3	-	6	24
1317000908010000	Port of Brunswick, GA	2	0	-	0	2
1318000902000000	Port of Jacksonville, FL	17	5	-	7	29

Organization Code	Location Title	Inspectors				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1318000902010000	Port of Fernandina, FL	1	0	-	0	2
1318000902020000	Port of Panama City, FL	1	0	-	0	2
1318000902030000	Port of Pensacola, FL	-	0	-	-	0
1318000903000000	Port of Orlando, FL	45	9	-	32	85
1318000903010000	Port of Port Canaveral, FL	13	3	-	9	26
1318000903020000	Sanford Regional Airport	8	0	-	7	16
1318000903840000	Daytona Beach Regional Airport	1	0	-	1	2
1318000903850000	Melbourne Regional Airport	1	0	-	0	2
1318000904000000	Port of Tampa, FL	28	6	-	4	38
1318000904010000	Port of St. Petersburg, FL	3	1	-	1	5
1318000904020000	Port of Manatee, FL	2	1	-	0	3
1318000904810000	Ft. Myers Regional Airport	4	1	-	1	5
1318000904830000	Sarasota Bradeton Airport	1	0	-	1	2
1320000900010000	Port of Mobile, AL	10	2	-	4	16
1320000900020000	Port of Gulfport, MS	4	1	-	1	6
1320000900030000	Port of Pascagoula, MS	2	0	-	0	3
1320000900040000	Port of Birmingham, AL	2	0	-	2	4
1320000900050000	Port of Huntsville, AL	4	1	-	1	5
1320000900060000	Port of New Orleans, LA	48	11	-	28	87
1320000900070000	Port of Memphis, TN	27	2	-	7	37
1320000900080000	Port of Baton Rouge, LA	4	1	-	1	6
1320000900090000	Port of Morgan City, LA	4	0	-	0	5
1320000900100000	Port of Little Rock, AK	2	1	-	1	3
1320000900110000	Port of Gramercy, LA	3	1	-	0	4
1320000900120000	Port of Greenville	-	-	-	-	-
1320000900130000	Port of Vicksburg, MS	3	0	-	1	4
1320000900140000	Port of Lake Charles, LA	4	1	-	1	6

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1320000900150000	Port of Shreveport-Bosier City, LA	2	0	-	0	3
1320000900160000	Port of Nashville, TN	10	2	-	2	14
1320000900170000	Port of Chattanooga, TN	2	1	-	0	3
1320000900180000	Port of Knoxville, TN	3	1	-	1	4
1323000900010000	Port of Brownsville, TX	155	23	-	96	275
1323000900020000	Port of Del Rio, TX	44	5	-	42	91
1323000900030000	Port of Eagle Pass, TX	61	9	-	63	132
1323000900040000	Port of Laredo, TX	253	60	-	135	448
1323000900050000	Port of Hidalgo, TX	134	15	-	112	261
1323000900060000	Port of Roma, TX	33	4	-	27	63
1323000900070000	Port of Rio Grande City, TX	22	4	-	10	35
1323000900090000	Port of Progreso, TX	28	3	-	28	59
1323000902000000	Port of San Antonio,TX	11	2	-	5	18
1323000902010000	Port of Austin, TX	3	1	-	0	4
1324000900010000	Port of El Paso, TX	319	47	-	251	617
1324000900020000	Port of Presidio, TX	25	3	-	26	54
1324000900030000	Port of Fabens, TX	18	2	-	19	39
1324000900040000	Port of Columbus, NM	21	3	-	13	37
1324000900050000	Port of Albuquerque, NM	5	1	-	1	6
1324000900060000	Port of Santa Teresa, NM	20	3	-	14	37
1325000900011000	Port of San Ysidro, CA	242	29	-	282	553
1325000900012000	Port of Otay Mesa , CA	135	31	-	43	209
1325000900020000	Port of Tecate, CA	20	4	-	12	36
1325000900030000	Port of Calexico, CA	167	37	-	111	314
1325000900040000	Port of Andrade, CA	16	1	-	16	33
1326000902000000	Port of Douglas, AZ	45	5	-	47	98
1326000902010000	Port of Naco, AZ	15	2	-	12	29

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1326000903000000	Port of Nogales, AZ	135	21	-	114	270
1326000903010000	Port of Sasabe, AZ	5	0	3	4	13
1326000904000000	Port of Phoenix, AZ	15	3	-	11	29
1326000904010000	Port of Tucson, AZ	8	1	-	5	15
1326000905000000	Port of San Luis, AZ	54	8	-	43	105
1326000905010000	Port of Lukeville, AZ	9	1	-	8	19
1327000901100000	Port of Long Beach, CA	147	34	-	36	217
1327000901200000	Port of LAX	360	40	-	294	694
1328000902000000	Port of San Francisco, CA	191	41	-	114	346
1328000902010000	Port of Eureka, CA	0	0	-	0	0
1328000902020000	Port of Fresno, CA	1	0	-	0	2
1328000902030000	Port of Reno, NV	3	1	-	0	4
1328000902040000	Port of Salt Lake City, UT	5	1	-	0	6
1328000902050000	Port of San Jose , CA	5	1	-	2	8
1328000903000000	Port of Honolulu, HI	123	21	-	76	221
1328000903010000	Port of Hilo, HI	5	1	-	2	7
1328000903020000	Port of Kahului, HI	2	0	-	1	4
1329000900010000	Port of Denver, CO	16	3	-	12	31
1329000900018200	Natrona County International Airport	0	0	-	0	1
1329000900018300	Jefferson Country Airport	1	-	-	1	2
1329000902000000	Port of Anchorage, AK	34	5	-	7	46
1329000902010000	Port of Juneau, AK	2	0	-	1	3
1329000902020000	Port of Ketchikan, AK	7	1	-	2	10
1329000902030000	Port of Skagway	3	0	4	3	10
1329000902040000	Port of Alcan, AK	7	1	-	4	13
1329000902050000	Port of Wrangell, AK	2	0	-	1	3
1329000902060000	Port of Dalton Cache, AK	3	0	5	3	11

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1329000902070000	Port of Valdez, AK	0	0	-	0	0
1329000902080000	Port of Fairbanks, AK	2	0	-	1	3
1329000902090000	Port of Sitka, AK	1	0	-	0	2
1329000902270000	Port of Kodiak, AK	-	-	-	-	-
1329000903000000	Port of Portland, OR	29	6	-	12	47
1329000903010000	Port of Astoria, OR	0	0	-	0	0
1329000903020000	Port of Newport, OR	0	0	-	0	1
1329000903030000	Port of Coos Bay, OR	1	0	-	0	2
1329000903040000	Port of Longview, WA	2	0	-	0	2
1329000903050000	Port of Boise, ID	1	0	-	0	2
1329000903820000	Rogue Valley-Medford User Fee Airport	1	0	-	1	2
1330000902000000	Port of Seattle, WA	88	19	-	53	159
1330000902010000	Port of Spokane, WA	2	0	-	2	4
1330000902820000	Grant County/Moses Lake User Fee Airport	1	0	-	1	2
1330000903000000	Port of Blaine, WA	71	11	-	60	142
1330000903010000	Port of Sumas, WA	21	4	-	15	40
1330000903020000	Port of Point Roberts, WA	1	0	7	1	10
1330000903030000	Port of Lynden, WA	12	1	-	8	21
1330000904000000	Port of Tacoma, WA	16	3	-	1	20
1330000904010000	Port of Aberdeen, WA	1	0	-	0	1
1330000904020000	Port of Bellinghham, WA	3	0	-	2	5
1330000904030000	Port of Everett, WA	1	0	-	0	1
1330000904040000	Port of Port Angeles, WA	9	1	-	7	17
1330000904050000	Port of Port Towsend, WA	1	0	-	1	2
1330000904060000	Port of Anacortes, WA	7	2	-	5	14
1330000904070000	Port of Friday Harbor, WA	7	1	-	4	11
1330000904090000	Port OF NEAH BAY, WA	-	-	-	-	-

Organization Code	Location Title	Inspectors				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000905000000	Port of Oroville, WA	13	2	1	9	26
1330000905020000	Port of Danville, WA	3	0	5	3	11
1330000905030000	Port of Ferry, WA	1	0	7	1	9
1330000905050000	Port of Laurier, WA	4	0	4	2	10
1330000905060000	Port of Frontier, WA	4	1	4	3	11
1330000905070000	Port of Metalme Falls, WA	3	0	5	2	10
1330000906000000	Port of Duluth, MN	4	0	-	3	8
1330000906010000	Port of Ashland, WI	-	-	-	-	-
1330000906020000	Port of International Falls/Ranier, MN	20	6	-	12	37
1330000906030000	PortPortage, MN	11	2	-	7	20
1330000907000000	Port of Great Falls, MT	5	1	2	3	11
1330000907010000	Port of Raymond, MT	8	1	-	3	12
1330000907020000	Port of Eastport, ID	8	2	7	3	20
1330000907030000	Port of Butte, MT	1	0	-	1	2
1330000907040000	Port of Turner, MT	1	0	7	1	9
1330000907050000	Port of Porthill, ID	4	1	4	3	11
1330000907060000	Port of Scobey, MT	1	0	7	1	9
1330000907070000	Port of Sweetgrass, MT	15	3	-	7	25
1330000907080000	Port of Whitetail, MT	1	0	7	1	9
1330000907090000	Port of Piegan, MT	5	1	2	4	12
1330000907100000	Port of Opheim, MT	1	0	7	1	9
1330000907110000	Port of Rooseville, MT	9	2	-	5	15
1330000907120000	Port of Morgan, MT	1	0	7	1	9
1330000907130000	Port of Whitlash, MT	1	0	7	1	9
1330000907140000	Port of Del Bonita, MT	1	0	7	1	9
1330000908000000	Port of Pembina, ND	32	9	-	20	60
1330000908020000	Port of Portal, ND	11	2	-	4	17

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000908030000	Port of Neche, ND	1	0	7	1	9
1330000908040000	Port of St. John, ND	1	0	7	0	9
1330000908050000	Port of Northgate, ND	1	0	7	1	9
1330000908060000	Port of Walhalla, ND	2	0	6	1	9
1330000908070000	Port of Hannah, ND	1	0	7	0	8
1330000908080000	Port of Sarles, ND	1	0	7	0	8
1330000908090000	Port of Ambrose, ND	1	0	7	1	9
1330000908100000	Port of Antler, ND	1	0	7	1	9
1330000908110000	Port of Sherwood, ND	1	0	7	1	9
1330000908120000	Port of Hansboro, ND	1	0	7	0	9
1330000908130000	Port of Maida, ND	1	0	7	0	9
1330000908140000	Port of Fortuna, ND	1	0	7	1	9
1330000908150000	Port of Westhope, ND	1	0	7	0	9
1330000908160000	Port of Noonan, ND	1	0	7	1	9
1330000908170000	Port of Carbury, ND	1	0	-	1	2
1330000908180000	Port of Dunseith, ND	6	1	1	4	12
1330000908190000	Port of Warroad, MN	6	1	1	5	13
1330000908200000	Port of Baudette, MN	7	1	-	7	15
1330000908220000	Port of Roseau, MN	3	0	5	2	11
1330000908810000	Hector User Fee Airport, Fargo	1	0	-	0	2
1338000900010000	Port of Detroit, MI	207	46	-	111	364
1338000900020000	Port of Port Huron, MI	65	21	-	15	100
1338000900030000	Port of Sault Sainte Marie, MI	22	5	-	9	36
1338000902000000	Port of Grand Rapids, MI	3	1	-	0	4
1338000902010000	Port of Battle Creek, MI	2	0	-	1	3
1338000902020000	Port of Saginaw/Bay City/Flint, MI	2	0	-	1	3
1338000902030000	Port of Muskegon, MI	-	-	-	-	-

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000900020000	Port of Kansas City	6	2	-	-	8
1339000900030000	Port of Cincinnati, OH/Lawrenceburg, IN	19	3	-	11	33
1339000900040000	Port of Columbus, OH	6	2	-	2	9
1339000900048200	Rickenbacker Airport	-	-	-	-	-
1339000900050000	Port of Dayton, OH	9	1	-	2	12
1339000900060000	Port of Toledo/Sandusky, OH	6	1	-	3	9
1339000900070000	Port of Louisville, KY	11	0	-	0	12
1339000900078400	Blue Grass Airport	1	0	-	0	1
1339000900080000	Port of Indianapolis, IN	12	1	-	3	17
1339000900088300	Baer Field Airport	1	0	-	0	1
1339000902000000	Port of Chicago, IL	157	32	-	86	275
1339000902010000	Port of Peoria, IL	1	0	-	0	1
1339000902020000	Port of Omaha, NE	1	0	-	0	2
1339000902030000	Port of Des Moines, IA	1	0	-	0	1
1339000902040000	Port of Davenport/Rock Island/Moline, IL	1	0	-	0	1
1339000902050000	Port of Rockford	2	0	-	1	4
1339000902810000	Waukegan Regional Airport	1	0	-	1	2
1339000902830000	Pal-Waukee Airport	1	-	-	1	2
1339000903000000	Port of Milwaukee, WI	5	1	-	1	7
1339000903020000	Port of Green Bay, WI	1	0	-	0	1
1339000903040000	PORT OF SHEBOYGAN, WI	-	-	-	-	-
1339000903050000	Port of Racine, WI	1	0	-	0	1
1339000904000000	Port of Cleveland, OH	12	2	-	12	25
1339000904010000	Port of Erie, PA	2	0	-	1	4
1339000904020000	Port of Owensboro, KY/Evansville, IN	1	0	-	-	1
1339000904030000	Port of Ashtabula/Comeaut, OH	1	0	-	0	1
1339000905000000	Port of St. Louis, MO	13	2	-	14	29

		Inspectors				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000905010000	PORT OF ST. JOSEPH, MO	-	-	-	-	-
1339000905020000	Port of Wichita, KA	2	0	-	0	3
1339000905030000	Port of Springfield, MO	1	0	-	0	1
1339000906000000	Port of Minneapolis, MN	31	6	-	20	56
1339000906010000	Port of Sioux Falls, SD	1	0	-	1	2
1339000906810000	Rochester User Fee Airport	1	0	-	1	2
1339000990010000	Vancouver, Canada Preclearance	20	4	-	20	44
1339000990020000	Calgary, Canada Preclearance	11	2	-	11	24
1339000990030000	Edmonton, Canada Preclearance	5	1	-	5	11
1339000990040000	Montreal, Canada Preclearance	21	4	-	22	46
1339000990050000	Toronto, Canada Preclearance	37	8	-	36	82
1339000990080000	Winnepeg, Canada Preclearance	6	1	-	6	13
1339000990090000	Ottawa, Canada Preclearance	6	1	-	6	13
1349000902000000	Port of San Juan, PR	139	29	-	93	260
1349000902020000	Port of Fajardo, PR	7	1	-	3	11
1349000902040000	Port of Huamaco, PR	-	-	-	-	-
1349000902050000	Port of Mayaguez, PR	6	2	-	4	12
1349000902060000	Port of Ponce, PR	4	1	-	1	5
1349000902070000	Port of Jobos, OR	-	-	-	-	-
1349000903000000	Port of Charlotte Amalie, VI	44	10	-	30	84
1349000903020000	PORT OF CORAL BAY VI	-	-	-	-	-
1349000903040000	PORT OF FREDERIKSTED VI	-	-	-	-	-
1352000900030000	Port of Port Everglades, FL	66	18	-	44	127
1352000900040000	Port of West Palm Beach, FL	26	5	-	16	47
1352000901010000	Miami Airport	420	57	-	385	862
1352000901020000	Miami Seaport	120	32	-	50	203
1352000990010000	Nassau, Bahamas	22	5	-	25	51

Organization Code	Location Title	Inspectors				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1352000990020000	Freeport, Bahamas	11	2	-	12	25
1352000990030000	Kindley Field, Bermuda	10	2	-	10	23
1353000902000000	Port of Corpus Christi, TX	3	0	-	0	4
1353000903000000	Port of Dallas/Ft. Worth, TX	97	14	-	122	232
1353000903010000	Port of Amarillo, TX	1	0	-	0	1
1353000903020000	Port of Lubbock, TX	1	0	-	0	1
1353000903040000	Port of Oklahoma City, OK	2	1	-	0	3
1353000903050000	Port of Tulsa, OK	2	0	-	0	3
1353000903820000	Midland Airport	1	0	-	0	2
1353000904000000	Port of Houston, TX	132	32	-	69	232
1353000904010000	Port of Port Author, TX	3	1	-	0	4
1353000904030000	Port of Freeport, TX	1	0	-	-	1
1400000001040000	Regulatory Audit Division	-	-	-	-	-
9999999999999999	Mission Support	102	18	-	-	120

Appendix K – Optimal Agent Staffing Levels by Location (Preliminary)

Note: When calculated to the location level, the optimal additional Agents required for enforcement threat (2,296) aggregate to a different number than when calculated globally (2,041). To remain consistent with the other global calculations, Customs chose the global calculation to include in its final staffing request.

		Agents				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
	Total:	2,363	-	-	2,296	4,659
0400000809010110	San Diego Aviation Branch	3	-	-	3	6
0400000809010111	Riverside Aviation Unit	0	-	-	0	0
0400000809010112	Sacramento Aviation Unit	-	-	-	-	-
0400000809010120	Tucson Aviation Branch	6	-	-	7	13
0400000809010121	Phoenix Aviation Unit	1	-	-	1	2
0400000809010130	Albuquerque Aviation Branch	5	-	-	6	12
0400000809010131	El Paso Aviation Unit	5	-	-	5	10
0400000809010140	San Angelo Aviation Branch	5	-	-	5	10
0400000809010141	San Antonio Unit	1	-	-	1	2
0400000809010200	Surv Sup Ctr(Corpus Chris, TX)	-	-	-	-	-
0400000809010201	PANAMA AVIATION UNIT	-	-	-	-	-
0400000809010310	Jacksonville Aviation Branch	4	-	-	5	9
0400000809010311	New York Aviation Unit	-	-	-	-	-
0400000809010312	Tampa Aviation Unit	0	-	-	0	0
0400000809010320	Houston Aviation Branch	2	-	-	3	5
0400000809010321	Kansas City	-	-	-	-	-
0400000809010330	New Orleans Aviation Branch	9	-	-	10	19
0400000809010331	Pensacola Aviation Branch	0	-	-	0	0

		Agents				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0400000809010332	Cincinnati Aviation Branch	-	-	-	-	-
0400000809010340	Miami Aviation Branch	5	-	-	6	10
0400000809010350	Puerto Rico Aviation Branch	3	-	-	3	6
0400000809010351	Gateway - Puerto Rico Air Branch	-	-	-	-	-
0400000809010500	Domestic Air Interdiction Coordination Center (DAICC)	0	-	-	0	1
0400000809010510	Drug Interdiction Ops Center	-	-	-	-	-
0400601600000000	CUST ATTACHE THE HAGUE NETH	-	-	-	-	-
0400601700000000	Senior Customs Rep - Interpol	0	-	-	-	0
0400601800000000	Customs Attache - Moscow	2	-	-	1	3
0400601900000000	Senior Customs Rep - Hong Kong BCC	3	-	-	2	5
0400602100000000	Customs Attache - London, Eng	2	-	-	2	5
0400602200000000	Customs Attache - Pretoria, South Africa	2	-	-	2	4
0400602500000000	Customs Attache - Mexico City, Mex	3	-	-	2	5
0400602800000000	Customs Attache - Ottawa, Canada	3	-	-	3	6
0400603200000000	Customs Attache - Paris, France	4	-	-	3	8
0400603400000000	Customs Attache - Rome, Italy	6	-	-	5	12
0400603500000000	Customs Attache - Panama City	1	-	-	1	1
0400603600000000	CUSTOMS ADVISOR PANAMA CITY	-	-	-	-	-
0400603700000000	Customs Attache - Tokyo, Japan	3	-	-	3	6
0400603800000000	Customs Attache - Bonn, Germany	5	-	-	4	9
0400603900000000	Customs Attache - Seoul, Korea	2	-	-	1	3
0400604000000000	Customs Attache - Bangkok, Thailand	2	-	-	1	3
0400604100000000	Customs Attache - Vienna, Austria	3	-	-	2	5
0400604300000000	CUSTOMS REP-MILAN, ITALY	-	-	-	-	-
0400604400000000	Customs Attache - Singapore	3	-	-	2	5
0400604500000000	CUSTOMS REP-MERIDA, MEXICO	18	-	-	20	38

		Agents				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0400604600000000	Customs Rep - Monterrey, Mexico	2	-	-	1	3
0400604700000000	Customs Rep - Tijuana, Mexico	1	-	-	1	2
0400604800000000	Customs Attache - Montevideo, UR	2	-	-	1	3
0400604900000000	Customs Attache - Miami, FL	1	-	-	0	1
0400605100000000	Customs Attache - Caracas, Venezuela	2	-	-	2	4
0400605200000000	Customs Attache - Beijing, China	3	-	-	2	5
0400605300000000	Customs Attache - Bogota, Colombia	0	-	-	0	0
0400605400000000	Customs Rep - Frankfurt	0	-	-	0	0
0400680000000000	Customs Communications Center	-	-	-	-	-
0404000000000000	SAC Boston	35	-	-	31	66
0404000001000000	RAC Bangor, ME	5	-	-	5	10
0404000002000000	RAC New Haven, CT	5	-	-	6	11
0404000003000000	RAC Burlington, VT	6	-	-	6	12
0409000000000000	SAC Buffalo, NY	21	-	-	19	41
0409000001000000	RAC Rouses Point, NY	13	-	-	12	25
0410000000000000	SAC New York, NY	81	-	-	66	147
0410000001000000	DSAC JFK International Airport	57	-	-	61	118
0410000001010000	RAC Long Island	19	-	-	16	35
0410000002000000	DSAC Newark, NJ	59	-	-	60	118
0410000003000000	DSAC World Trade Center	20	-	-	-	20
0413000000000000	SAC Baltimore	30	-	-	28	57
0413000001000000	RAC Philadelphia, PA	41	-	-	39	81
0413000002000000	RAC Washington, DC	26	-	-	26	53
0417000000000000	SAC Atlanta	29	-	-	26	55
0417000001000000	RAC Charleston, SC	10	-	-	10	20
0417000002000000	RAC Charlotte, NC	15	-	-	14	29
0417000003000000	RAC Savannah, GA	7	-	-	8	15

Organization Code	Location Title	Agents				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0417000004000000	RAC Greenville, SC	8	-	-	6	14
0417000005000000	RAC Norfolk, VA	14	-	-	14	28
0417000006000000	RAC Wilmington, NC	9	-	-	9	18
0418000000000000	SAC Tampa, FL	59	-	-	60	119
0418000001000000	RAC Port Canaveral, FL	7	-	-	5	12
0418000002000000	RAC Ft Myers, FL	17	-	-	16	33
0418000003000000	RAC Jacksonville, FL	13	-	-	14	27
0418000004000000	RAC Orlando, FL	18	-	-	16	34
0418000005000000	RAC Panama City, FL	6	-	-	6	12
0418000006000000	RAC Pensacola, FL	9	-	-	9	18
0418000007000000	RAC Tallahassee, FL	7	-	-	7	14
0418000008000000	RAC Sarasota, FL	6	-	-	7	13
0420000000000000	SAC New Orleans	54	-	-	53	107
0420000001000000	RAC Lafayette, LA	7	-	-	6	13
0420000002000000	RAC Baton Rouge, LA	5	-	-	5	10
0420000003000000	RAC Lake Charles	4	-	-	4	8
0420000004000000	RAC Shreveport, LA	4	-	-	4	9
0420000005000000	RAC Little Rock, AR	3	-	-	3	6
0420000006000000	RAC Houma, LA	6	-	-	6	12
0420000007000000	RAC Gulfport, MS	13	-	-	14	28
0420000008000000	RAC Mobile	21	-	-	22	43
0420000009000000	RAC Memphis	6	-	-	5	11
0420000010000000	RAC Gulf Shores, AL	5	-	-	5	9
0420000011000000	RAC Birmingham, AL	5	-	-	5	11
0420000012000000	RAC Nashville, TN	7	-	-	7	15
0423000000000000	SAC San Antonio, TX	23	-	-	23	46
0423000001000000	RAC Brownsville, TX	33	-	-	37	69

		Agents				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0423000002000000	RAC San Angelo/Midland, TX	8	-	-	10	18
0423000003000000	RAC Mc Allen, TX	5	-	-	-	5
0423000004000000	RAC Laredo, TX	27	-	-	30	56
0423000005000000	RAC Falcon Dam,TX	5	-	-	6	11
0423000006000000	RAC Eagle Pass, TX	8	-	-	9	17
0423000007000000	RAC Del Rio, TX	7	-	-	8	16
0424000000000000	SAC El Paso, TX	60	-	-	68	128
0424000001000000	RAC Albuquerque, NM	10	-	-	11	21
0424000002000000	RAC Deming, NM	11	-	-	13	24
0424000003000000	RAC Las Cruces, NM	12	-	-	14	26
0424000004000000	RAC Alpine	4	-	-	4	8
0425000000000000	SAC San Diego	70	-	-	71	141
0425000001000000	RAC Oceanside, CA	6	-	-	7	13
0425000002000000	RAC Calexico, CA	28	-	-	33	61
0425000003000000	RAC San Ysidro, CA	55	-	-	66	122
0426000000000000	SAC Tucson	34	-	-	35	69
0426000001000000	RAC Phoenix, AZ	10	-	-	9	19
0426000002000000	RAC Douglas, AZ	15	-	-	18	33
0426000003000000	RAC Nogalas, AZ	26	-	-	29	55
0426000004000000	RAC Sellis, AZ	14	-	-	16	30
0426000005000000	RAC Yuma, AZ	14	-	-	16	30
0427000000000000	SAC Los Angeles, CA	70	-	-	55	125
0427000001000000	RAC Los Angeles Intl Airport	18	-	-	17	35
0427000002000000	RAC Riverside, CA	14	-	-	13	27
0427000003000000	RAC Orange County, CA	7	-	-	7	14
0427000004000000	RAC Oxnard, CA	6	-	-	7	13
0427000005000000	RAC Las Vegas, NV	7	-	-	6	13

Organization Code	Location Title	Agents				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0428000000000000	SAC San Francisco, CA	29	-	-	27	56
0428000001000000	RAC San Francisco Intl Airport	9	-	-	9	18
0428000002000000	RAC San Jose, CA	11	-	-	9	20
0428000003000000	RAC Sacramento, CA	8	-	-	8	17
0428000004000000	RAC Honolulu, HI	16	-	-	15	31
0428000005000000	RAC Salt Lake City	4	-	-	5	9
0429000000000000	SAC Denver	16	-	-	16	33
0429000001000000	RAC Portland, OR	12	-	-	12	24
0430000000000000	SAC Seattle	25	-	-	22	47
0430000001000000	RAC Seattle-Tacoma, WA	6	-	-	6	12
0430000002000000	RAC Blaine, WA	18	-	-	18	36
0430000003000000	RAC Great Falls, MT	7	-	-	7	13
0438000000000000	SAC Detroit	36	-	-	33	69
0439000000000000	SAC Chicago	42	-	-	36	78
0439000001000000	RAC Minneapolis, MN	14	-	-	13	27
0439000002000000	RAC Cleveland, OH	17	-	-	14	31
0439000003000000	RAC Cincinnati, OH	6	-	-	5	11
0439000004000000	RAC St. Louis, MO	5	-	-	5	10
0439000005000000	RAC Kansas City, MO	7	-	-	6	13
0439000006000000	RAC Indianapolis, IN	5	-	-	4	9
0449000000000000	SAC San Juan, PR	49	-	-	46	95
0449000001000000	RAC Fajardo, PR	5	-	-	6	11
0449000002000000	RAC Mayaguez, PR	10	-	-	10	20
0449000003000000	RAC Ponce, PR	4	-	-	5	9
0449000004000000	RAC St. Thomas, VI	3	-	-	4	7
0452000000000000	SAC Miami, FL	145	-	-	145	290
0452000001000000	RAC Ft. Lauderdale, FL	21	-	-	23	45

Organization Code	Location Title	Agents				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
04520000002000000	RAC Ft. Pierce, FL	7	-	-	7	14
04520000003000000	RAC Key Largo, FL	7	-	-	8	16
04520000004000000	RAC Key West, FL	13	-	-	14	26
04520000005000000	RAC West Palm Beach, FL	14	-	-	13	27
04530000000000000	SAC Houston	79	-	-	71	150
04530000001000000	RAC Galveston, TX	9	-	-	10	19
04530000002000000	RAC Corpus Christi, TX	13	-	-	14	28
04530000003000000	RAC Dallas, TX	36	-	-	34	70
99999999999999	Mission Support	130	-	-	114	244

Appendix L – Optimal CEO Staffing Levels by Location (Preliminary)

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
	Total:	641	34	-	616	1,291
1304000900010000	Port of St. Albans, VT	-	-	-	-	-
1304000902000000	Port of Portland, ME	-	0	-	-	0
1304000902010000	Port of Jackman, ME	-	-	-	-	-
1304000902020000	Port of Bangor, ME	-	-	-	-	-
1304000902030000	Port of Bath, ME	-	-	-	-	-
1304000902040000	Port of Bar Harbor, ME	-	-	-	-	-
1304000902050000	Port of Rockland, ME	-	-	-	-	-
1304000902060000	Port of Portsmouth, NH	-	-	-	-	-
1304000903000000	Port of Calais, ME	-	-	-	-	-
1304000903010000	Port of Eastport, ME	-	-	-	-	-
1304000903020000	Port of Vanceboro, ME	-	-	-	-	-
1304000903030000	Port of Jonesport, ME	-	-	-	-	-
1304000904000000	Port of Houlton, ME	1	0	-	1	2
1304000904010000	Port of Van Buren, ME	-	-	-	-	-
1304000904020000	Port of Madawaska, ME	-	-	-	-	-
1304000904030000	Port of Fort Kent, ME	-	-	-	-	-
1304000905000000	Port of Highgate Springs/Alburg, VT	1	0	-	1	2
1304000905010000	Port of Richford, VT	-	-	-	-	-
1304000905020000	Port of Burlington, VT	-	-	-	-	-
1304000906000000	Port of Derby Line, VT	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1304000906010000	Port of Norton-Beecher Falls, VT	-	-	-	-	-
1304000907000000	Port of Boston, MA	3	0	-	3	6
1304000907010000	Port of Springfield, MA	-	-	-	-	-
1304000907020000	Port of Worcester, MA	-	-	-	-	-
1304000907030000	Port of Gloucester, MA	-	-	-	-	-
1304000907040000	Port of New Bedford, MA	-	-	-	-	-
1304000908000000	Port of Hartford, CT	-	-	-	-	-
1304000908010000	Port of Bridgeport, CT	1	0	-	1	2
1304000908020000	Port of New Haven, CT	-	0	-	-	0
1304000909000000	Port of Providence, RI	-	-	-	-	-
1304000909010000	Port of Newport, RI	-	-	-	-	-
1309000900010000	Port of Albany, NY	-	-	-	-	-
1309000902000000	Port of Champlain-Rouses Point, NY	2	0	-	2	4
1309000902010000	Port of Trout River/Chateaugay/Ft. Covington	-	0	-	-	0
1309000903000000	Port of Ogdensburg, NY	1	0	-	1	2
1309000903020000	Port of Cape Vincent, NY	-	-	-	-	-
1309000903040000	Port of Clayton, NY	-	-	-	-	-
1309000904000000	Port of Buffalo, NY	3	0	-	3	6
1309000904040000	Port of Syracuse, NY	-	-	-	-	-
1310000901000000	Port of New York-Newark	13	1	-	12	26
1310000902000000	Port of JFK Airport	22	1	-	21	44
1313000900030000	Port of Chester, PA / Wilmington, DE	-	-	-	-	-
1313000900040000	Port of Pittsburgh, PA	-	-	-	-	-
1313000900050000	Port of Washington, DC	4	0	-	4	8
1313000900060000	Port of Alexandria, VA	-	-	-	-	-
1313000902000000	Port of Baltimore, MD	2	0	-	2	4
1313000902020000	PORT OF CAMBRIDGE, MD	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1313000902030000	PORT OF CRISFIELD MD	-	-	-	-	-
1313000903000000	Port of Harrisburg, PA	-	-	-	-	-
1313000903010000	Port of Wilkes Barre/Scranton, PA	-	-	-	-	-
1313000941000000	Port of Philadelphia, PA	3	0	-	3	6
1313000941008200	Atlantic City User Fee Airport	-	-	-	-	-
1313000941010000	Port of Lehigh Valley, PA	-	-	-	-	-
1317000900010000	Port of Charlotte, NC	-	-	-	-	-
1317000900020000	Port of Charleston, SC	-	-	-	-	-
1317000900030000	Port of Atlanta, GA	7	0	-	7	14
1317000902000000	Port of Norfolk, VA	-	-	-	-	-
1317000902010000	Port of Newport News, VA	-	-	-	-	-
1317000903000000	Port of Richmond-Petersburg, VA	-	-	-	-	-
1317000903010000	Port of Charleston, WV	-	-	-	-	-
1317000903020000	Port of Front Royal, VA	-	-	-	-	-
1317000904000000	Port of Wilmington, NC	-	-	-	-	-
1317000904010000	Port of Reidsville, NC	-	-	-	-	-
1317000904020000	Port of Beaufort-Morehead, NC	-	-	-	-	-
1317000905000000	Port of Durham, NC	-	-	-	-	-
1317000905010000	Port of Winston Salem, NC	-	-	-	-	-
1317000907000000	Port of Greenville-Spartanburg, SC	-	-	-	-	-
1317000907010000	Port of Georgetown, SC	-	-	-	-	-
1317000907020000	Port of Columbia, SC	-	-	-	-	-
1317000908000000	Port of Savannah, GA	-	-	-	-	-
1317000908010000	Port of Brunswick, GA	-	-	-	-	-
1318000902000000	Port of Jacksonville, FL	2	0	-	2	4
1318000902010000	Port of Fernandina, FL	-	0	-	-	0
1318000902020000	Port of Panama City, FL	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1318000902030000	Port of Pensacola, FL	-	-	-	-	-
1318000903000000	Port of Orlando, FL	2	0	-	2	4
1318000903010000	Port of Port Canaveral, FL	1	0	-	1	2
1318000903020000	Sanford Regional Airport	-	-	-	-	-
1318000903840000	Daytona Beach Regional Airport	-	-	-	-	-
1318000903850000	Melbourne Regional Airport	-	-	-	-	-
1318000904000000	Port of Tampa, FL	1	0	-	1	2
1318000904010000	Port of St. Petersburg, FL	-	-	-	-	-
1318000904020000	Port of Manatee, FL	-	-	-	-	-
1318000904810000	Ft. Myers Regional Airport	-	-	-	-	-
1318000904830000	Sarasota Bradeton Airport	-	-	-	-	-
1320000900010000	Port of Mobile, AL	1	0	-	1	2
1320000900020000	Port of Gulfport, MS	-	0	-	-	0
1320000900030000	Port of Pascagoula, MS	-	0	-	-	0
1320000900040000	Port of Birmingham, AL	-	0	-	-	0
1320000900050000	Port of Huntsville, AL	-	-	-	-	-
1320000900060000	Port of New Orleans, LA	5	0	-	5	10
1320000900070000	Port of Memphis, TN	3	0	-	3	6
1320000900080000	Port of Baton Rouge, LA	-	-	-	-	-
1320000900090000	Port of Morgan City, LA	-	-	-	-	-
1320000900100000	Port of Little Rock, AK	-	-	-	-	-
1320000900110000	Port of Gramercy, LA	-	0	-	-	0
1320000900120000	Port of Greenville	-	-	-	-	-
1320000900130000	Port of Vicksburg, MS	-	-	-	-	-
1320000900140000	Port of Lake Charles, LA	1	0	-	1	2
1320000900150000	Port of Shreveport-Bosier City, LA	-	-	-	-	-
1320000900160000	Port of Nashville, TN	-	0	-	-	0

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1320000900170000	Port of Chattanooga, TN	-	-	-	-	-
1320000900180000	Port of Knoxville, TN	-	-	-	-	-
1323000900010000	Port of Brownsville, TX	27	1	-	26	54
1323000900020000	Port of Del Rio, TX	7	0	-	7	14
1323000900030000	Port of Eagle Pass, TX	13	0	-	12	26
1323000900040000	Port of Laredo, TX	49	2	-	47	98
1323000900050000	Port of Hidalgo, TX	33	1	-	32	66
1323000900060000	Port of Roma, TX	9	0	-	9	18
1323000900070000	Port of Rio Grande City, TX	-	0	-	-	0
1323000900090000	Port of Progreso, TX	5	0	-	5	10
1323000902000000	Port of San Antonio, TX	2	0	-	2	4
1323000902010000	Port of Austin, TX	-	-	-	-	-
1324000900010000	Port of El Paso, TX	55	3	-	53	110
1324000900020000	Port of Presidio, TX	4	0	-	4	8
1324000900030000	Port of Fabens, TX	2	0	-	2	4
1324000900040000	Port of Columbus, NM	6	0	-	6	12
1324000900050000	Port of Albuquerque, NM	1	0	-	1	2
1324000900060000	Port of Santa Teresa, NM	2	-	-	2	4
1325000900011000	Port of San Ysidro, CA	65	2	-	62	130
1325000900012000	Port of Otay Mesa, CA	-	0	-	-	0
1325000900020000	Port of Tecate, CA	10	0	-	10	20
1325000900030000	Port of Calexico, CA	29	1	-	28	58
1325000900040000	Port of Andrade, CA	5	0	-	5	10
1326000902000000	Port of Douglas, AZ	13	1	-	12	26
1326000902010000	Port of Naco, AZ	-	0	-	-	0
1326000903000000	Port of Nogales, AZ	31	1	-	30	62
1326000903010000	Port of Sasabe, AZ	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1326000904000000	Port of Phoenix, AZ	2	0	-	2	4
1326000904010000	Port of Tucson, AZ	-	-	-	-	-
1326000905000000	Port of San Luis, AZ	19	1	-	18	38
1326000905010000	Port of Lukeville, AZ	-	-	-	-	-
1327000901100000	Port of Long Beach, CA	4	0	-	4	8
1327000901200000	Port of LAX	17	0	-	16	34
1328000902000000	Port of San Francisco, CA	3	4	-	3	10
1328000902010000	Port of Eureka, CA	-	-	-	-	-
1328000902020000	Port of Fresno, CA	-	-	-	-	-
1328000902030000	Port of Reno, NV	-	-	-	-	-
1328000902040000	Port of Salt Lake City, UT	-	-	-	-	-
1328000902050000	Port of San Jose, CA	-	-	-	-	-
1328000903000000	Port of Honolulu, HI	6	0	-	6	12
1328000903010000	Port of Hilo, HI	1	0	-	1	2
1328000903020000	Port of Kahului, HI	-	-	-	-	-
1329000900010000	Port of Denver, CO	1	0	-	1	2
1329000900018200	Natrona County International Airport	-	-	-	-	-
1329000900018300	Jefferson Country Airport	-	-	-	-	-
1329000902000000	Port of Anchorage, AK	-	-	-	-	-
1329000902010000	Port of Juneau, AK	-	-	-	-	-
1329000902020000	Port of Ketchikan, AK	-	-	-	-	-
1329000902030000	Port of Skagway	-	-	-	-	-
1329000902040000	Port of Alcan, AK	-	-	-	-	-
1329000902050000	Port of Wrangell, AK	-	-	-	-	-
1329000902060000	Port of Dalton Cache, AK	-	-	-	-	-
1329000902070000	Port of Valdez, AK	-	-	-	-	-
1329000902080000	Port of Fairbanks, AK	-	-	-	-	-

		CEOs				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1329000902090000	Port of Sitka, AK	-	-	-	-	-
1329000902270000	Port of Kodiak, AK	-	-	-	-	-
1329000903000000	Port of Portland, OR	1	0	-	1	2
1329000903010000	Port of Astoria, OR	-	-	-	-	-
1329000903020000	Port of Newport, OR	-	-	-	-	-
1329000903030000	Port of Coos Bay, OR	-	-	-	-	-
1329000903040000	Port of Longview, WA	-	-	-	-	-
1329000903050000	Port of Boise, ID	-	-	-	-	-
1329000903820000	Rogue Valley-Medford User Fee Airport	-	-	-	-	-
1330000902000000	Port of Seattle, WA	7	0	-	7	14
1330000902010000	Port of Spokane, WA	-	-	-	-	-
1330000902820000	Grant County/Moses Lake User Fee Airport	-	-	-	-	-
1330000903000000	Port of Blaine, WA	5	0	-	5	10
1330000903010000	Port of Sumas, WA	-	0	-	-	0
1330000903020000	Port of Point Roberts, WA	-	-	-	-	-
1330000903030000	Port of Lynden, WA	-	0	-	-	0
1330000904000000	Port of Tacoma, WA	-	0	-	-	0
1330000904010000	Port of Aberdeen, WA	-	-	-	-	-
1330000904020000	Port of Bellinghham, WA	-	-	-	-	-
1330000904030000	Port of Everett, WA	-	-	-	-	-
1330000904040000	Port of Port Angeles, WA	-	-	-	-	-
1330000904050000	Port of Port Towsend, WA	-	-	-	-	-
1330000904060000	Port of Anacortes, WA	-	0	-	-	0
1330000904070000	Port of Friday Harbor, WA	-	-	-	-	-
1330000904090000	Port OF NEAH BAY,WA	-	-	-	-	-
1330000905000000	Port of Oroville, WA	1	0	-	1	2
1330000905020000	Port of Danville, WA	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000905030000	Port of Ferry, WA	-	-	-	-	-
1330000905050000	Port of Laurier, WA	-	-	-	-	-
1330000905060000	Port of Frontier, WA	-	-	-	-	-
1330000905070000	Port of Metaline Falls, WA	-	-	-	-	-
1330000906000000	Port of Duluth, MN	-	-	-	-	-
1330000906010000	Port of Ashland, WI	-	-	-	-	-
1330000906020000	Port of International Falls/Ranier, MN	-	-	-	-	-
1330000906030000	PortPortage, MN	-	-	-	-	-
1330000907000000	Port of Great Falls, MT	-	-	-	-	-
1330000907010000	Port of Raymond, MT	-	-	-	-	-
1330000907020000	Port of Eastport, ID	-	-	-	-	-
1330000907030000	Port of Butte, MT	-	-	-	-	-
1330000907040000	Port of Turner, MT	-	-	-	-	-
1330000907050000	Port of Porthill, ID	-	-	-	-	-
1330000907060000	Port of Scobey, MT	-	-	-	-	-
1330000907070000	Port of Sweetgrass, MT	1	0	-	1	2
1330000907080000	Port of Whitetail, MT	-	-	-	-	-
1330000907090000	Port of Piegan, MT	-	-	-	-	-
1330000907100000	Port of Opheim, MT	-	-	-	-	-
1330000907110000	Port of Rooseville, MT	-	-	-	-	-
1330000907120000	Port of Morgan, MT	-	-	-	-	-
1330000907130000	Port of Whitlash, MT	-	-	-	-	-
1330000907140000	Port of Del Bonita, MT	-	-	-	-	-
1330000908000000	Port of Pembina, ND	1	0	-	1	2
1330000908020000	Port of Portal, ND	-	0	-	-	0
1330000908030000	Port of Neche, ND	-	-	-	-	-
1330000908040000	Port of St. John, ND	-	-	-	-	-

		CEOs				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000908050000	Port of Northgate, ND	-	-	-	-	-
1330000908060000	Port of Walhalla, ND	-	0	-	-	0
1330000908070000	Port of Hannah, ND	-	-	-	-	-
1330000908080000	Port of Sarles, ND	-	-	-	-	-
1330000908090000	Port of Ambrose, ND	-	-	-	-	-
1330000908100000	Port of Antler, ND	-	-	-	-	-
1330000908110000	Port of Sherwood, ND	-	-	-	-	-
1330000908120000	Port of Hansboro, ND	-	-	-	-	-
1330000908130000	Port of Maida, ND	-	-	-	-	-
1330000908140000	Port of Fortuna, ND	-	-	-	-	-
1330000908150000	Port of Westhope, ND	-	-	-	-	-
1330000908160000	Port of Noonan, ND	-	-	-	-	-
1330000908170000	Port of Carbury, ND	-	-	-	-	-
1330000908180000	Port of Dunseith, ND	-	-	-	-	-
1330000908190000	Port of Warroad, MN	-	0	-	-	0
1330000908200000	Port of Baudette, MN	-	0	-	-	0
1330000908220000	Port of Roseau, MN	-	0	-	-	0
1330000908810000	Hector Uset. Fee Airport, Fargo	-	-	-	-	-
1338000900010000	Port of Detroit, MI	4	0	-	4	8
1338000900020000	Port of Port Huron, MI	-	-	-	-	-
1338000900030000	Port of Sault Sainte Marie, MI	-	0	-	-	0
1338000902000000	Port of Grand Rapids, MI	-	-	-	-	-
1338000902010000	Port of Battle Creek, MI	-	-	-	-	-
1338000902020000	Port of Saginaw/Bay City/Flint, MI	-	-	-	-	-
1338000902030000	Port of Muskegon, MI	-	-	-	-	-
1339000900020000	Port of Kansas City	-	-	-	-	-
1339000900030000	Port of Cincinnati, OH/Lawrenceburg, IN	2	0	-	2	4

		CEOs				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000900040000	Port of Columbus, OH	-	-	-	-	-
1339000900048200	Rickenbacker Airport	-	-	-	-	-
1339000900050000	Port of Dayton, OH	1	-	-	1	2
1339000900060000	Port of Toledo/Sandusky, OH	-	-	-	-	-
1339000900070000	Port of Louisville, KY	-	-	-	-	-
1339000900078400	Blue Grass Airport	-	-	-	-	-
1339000900080000	Port of Indianapolis, IN	1	0	-	1	2
1339000900088300	Baer Field Airport	-	-	-	-	-
1339000902000000	Port of Chicago, IL	8	0	-	8	16
1339000902010000	Port of Peoria, IL	-	-	-	-	-
1339000902020000	Port of Omaha, NE	-	-	-	-	-
1339000902030000	Port of Des Moines, IA	-	-	-	-	-
1339000902040000	Port of Davenport/Rock Island/Moline, IL	-	-	-	-	-
1339000902050000	Port of Rockford	-	-	-	-	-
1339000902810000	Waukegan Regional Airport	-	-	-	-	-
1339000902830000	Pal-Waukee Airport	-	-	-	-	-
1339000903000000	Port of Milwaukee, WI	-	-	-	-	-
1339000903020000	Port of Green Bay, WI	-	-	-	-	-
1339000903040000	PORT OF SHEBOYGAN, WI	-	-	-	-	-
1339000903050000	Port of Racine, WI	-	-	-	-	-
1339000904000000	Port of Cleveland, OH	-	-	-	-	-
1339000904010000	Port of Erie, PA	-	-	-	-	-
1339000904020000	Port of Owensboro, KY/Evansville, IN	-	-	-	-	-
1339000904030000	Port of Ashtabula/Conneaut, OH	-	-	-	-	-
1339000905000000	Port of St. Louis, MO	1	0	-	1	2
1339000905010000	PORT OF ST. JOSEPH, MO	-	-	-	-	-
1339000905020000	Port of Wichita, KA	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000905030000	Port of Springfield, MO	-	-	-	-	-
1339000906000000	Port of Minneapolis, MN	1	0	-	1	2
1339000906010000	Port of Sioux Falls, SD	-	-	-	-	-
1339000906810000	Rochester User Fee Airport	-	-	-	-	-
1339000990010000	Vancouver, Canada Preclearance	2	0	-	2	4
1339000990020000	Calgary, Canada Preclearance	2	0	-	2	4
1339000990030000	Edmonton, Canada Preclearance	-	0	-	-	0
1339000990040000	Montreal, Canada Preclearance	-	0	-	-	0
1339000990050000	Toronto, Canada Preclearance	1	0	-	1	2
1339000990080000	Winnepeg, Canada Preclearance	-	-	-	-	-
1339000990090000	Ottawa, Canada Preclearance	-	-	-	-	-
1349000902000000	Port of San Juan, PR	13	1	-	12	26
1349000902020000	Port of Fajardo, PR	1	-	-	1	2
1349000902040000	Port of Huamaco, PR	-	-	-	-	-
1349000902050000	Port of Mayaguez, PR	-	0	-	-	0
1349000902060000	Port of Ponce, PR	-	0	-	-	0
1349000902070000	Port of Jobos, OR	-	-	-	-	-
1349000903000000	Port of Charlotte Amalie, VI	-	0	-	-	0
1349000903020000	PORT OF CORAL BAY VI	-	-	-	-	-
1349000903040000	PORT OF FREDERIKSTED VI	-	-	-	-	-
1352000900030000	Port of Port Everglades, FL	2	0	-	2	4
1352000900040000	Port of West Palm Beach, FL	-	0	-	-	0
1352000901010000	Miami Airport	49	2	-	47	98
1352000901020000	Miami Seaport	-	3	-	-	3
1352000990010000	Nassau, Bahamas	-	-	-	-	-
1352000990020000	Freeport, Bahamas	-	-	-	-	-
1352000990030000	Kindley Field, Bermuda	-	-	-	-	-

Organization Code	Location Title	CEOs				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1353000902000000	Port of Corpus Christi, TX	-	-	-	-	-
1353000903000000	Port of Dallas/Ft. Worth, TX	2	0	-	2	4
1353000903010000	Port of Amarillo, TX	-	-	-	-	-
1353000903020000	Port of Lubbock, TX	-	-	-	-	-
1353000903040000	Port of Oklahoma City, OK	-	-	-	-	-
1353000903050000	Port of Tulsa, OK	-	-	-	-	-
1353000903820000	Midland Airport	-	-	-	-	-
1353000904000000	Port of Houston, TX	17	1	-	16	34
1353000904010000	Port of Port Author, TX	-	-	-	-	-
1353000904030000	Port of Freeport, TX	-	-	-	-	-
1400000001040000	Regulatory Audit Division	-	-	-	-	-
9999999999999999	Mission Support	18	1	-	17	36

Appendix M – Optimal Import Specialist Staffing Levels by Location (Preliminary)

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
	Total:	1,249	240	-	-	1,489
1304000900010000	Port of St. Albans, VT	12	1	-	-	13
1304000902000000	Port of Portland, ME	6	1	-	-	7
1304000902010000	Port of Jackman, ME	-	-	-	-	-
1304000902020000	Port of Bangor, ME	-	-	-	-	-
1304000902030000	Port of Bath, ME	-	-	-	-	-
1304000902040000	Port of Bar Harbor, ME	-	-	-	-	-
1304000902050000	Port of Rockland, ME	-	-	-	-	-
1304000902060000	Port of Portsmouth, NH	-	-	-	-	-
1304000903000000	Port of Calais, ME	-	-	-	-	-
1304000903010000	Port of Eastport, ME	-	-	-	-	-
1304000903020000	Port of Vanceboro, ME	-	-	-	-	-
1304000903030000	Port of Jonesport, ME	-	-	-	-	-
1304000904000000	Port of Houlton, ME	-	-	-	-	-
1304000904010000	Port of Van Buren, ME	-	-	-	-	-
1304000904020000	Port of Madawaska, ME	-	-	-	-	-
1304000904030000	Port of Fort Kent, ME	-	-	-	-	-
1304000905000000	Port of Highgate Springs/Alburg, VT	-	-	-	-	-
1304000905010000	Port of Richford, VT	-	-	-	-	-
1304000905020000	Port of Burlington, VT	-	-	-	-	-

Organization Code	Location Title	Import Specialists				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1304000906000000	Port of Derby Line, VT	-	-	-	-	-
1304000906010000	Port of Norton-Beecher Falls, VT	-	-	-	-	-
1304000907000000	Port of Boston, MA	30	8	-	-	37
1304000907010000	Port of Springfield, MA	-	-	-	-	-
1304000907020000	Port of Worcester, MA	-	-	-	-	-
1304000907030000	Port of Gloucester, MA	-	-	-	-	-
1304000907040000	Port of New Bedford, MA	-	-	-	-	-
1304000908000000	Port of Hartford, CT	2	0	-	-	2
1304000908010000	Port of Bridgeport, CT	-	-	-	-	-
1304000908020000	Port of New Haven, CT	-	-	-	-	-
1304000909000000	Port of Providence, RI	2	1	-	-	3
1304000909010000	Port of Newport, RI	-	-	-	-	-
1309000900010000	Port of Albany, NY	-	-	-	-	-
1309000902000000	Port of Champlain-Rouses Point, NY	26	4	-	-	30
1309000902010000	Port of Trout River/Chateaugay/Ft. Covington	-	-	-	-	-
1309000903000000	Port of Ogdensburg, NY	-	-	-	-	-
1309000903020000	Port of Cape Vincent, NY	-	-	-	-	-
1309000903040000	Port of Clayton, NY	-	-	-	-	-
1309000904000000	Port of Buffalo, NY	49	9	-	-	58
1309000904040000	Port of Syracuse, NY	-	-	-	-	-
1310000901000000	Port of New York-Newark	92	20	-	-	112
1310000902000000	Port of JFK Airport	141	23	-	-	164
1313000900030000	Port of Chester, PA / Wilmington, DE	-	-	-	-	-
1313000900040000	Port of Pittsburgh, PA	1	0	-	-	1
1313000900050000	Port of Washington, DC	5	1	-	-	6
1313000900060000	Port of Alexandria, VA	-	-	-	-	-
1313000902000000	Port of Baltimore, MD	19	4	-	-	23

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1313000902020000	PORT OF CAMBRIDGE, MD	-	-	-	-	-
1313000902030000	PORT OF CRISFIELD MD	-	-	-	-	-
1313000903000000	Port of Harrisburg, PA	-	-	-	-	-
1313000903010000	Port of Wilkes Barre/Scranton, PA	-	-	-	-	-
1313000941000000	Port of Philadelphia, PA	22	5	-	-	27
1313000941008200	Atlantic City User Fee Airport	-	-	-	-	-
1313000941010000	Port of Lehigh Valley, PA	-	-	-	-	-
1317000900010000	Port of Charlotte, NC	8	1	-	-	9
1317000900020000	Port of Charleston, SC	14	3	-	-	17
1317000900030000	Port of Atlanta, GA	15	2	-	-	17
1317000902000000	Port of Norfolk, VA	10	2	-	-	12
1317000902010000	Port of Newport News, VA	-	-	-	-	-
1317000903000000	Port of Richmond-Petersburg, VA	-	-	-	-	-
1317000903010000	Port of Charleston, WV	-	-	-	-	-
1317000903020000	Port of Front Royal, VA	-	-	-	-	-
1317000904000000	Port of Wilmington, NC	-	-	-	-	-
1317000904010000	Port of Reidsville, NC	-	-	-	-	-
1317000904020000	Port of Beaufort-Morehead, NC	-	-	-	-	-
1317000905000000	Port of Durham, NC	-	-	-	-	-
1317000905010000	Port of Winston Salem, NC	-	-	-	-	-
1317000907000000	Port of Greenville-Spartanburg, SC	-	-	-	-	-
1317000907010000	Port of Georgetown, SC	-	-	-	-	-
1317000907020000	Port of Columbia, SC	-	-	-	-	-
1317000908000000	Port of Savannah, GA	6	1	-	-	7
1317000908010000	Port of Brunswick, GA	-	-	-	-	-
1318000902000000	Port of Jacksonville, FL	5	1	-	-	6
1318000902010000	Port of Fernandina, FL	-	-	-	-	-

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1318000902020000	Port of Panama City, FL	-	-	-	-	-
1318000902030000	Port of Pensacola, FL	-	-	-	-	-
1318000903000000	Port of Orlando, FL	1	0	-	-	1
1318000903010000	Port of Port Canaveral, FL	-	-	-	-	-
1318000903020000	Sanford Regional Airport	-	-	-	-	-
1318000903840000	Daytona Beach Regional Airport	-	-	-	-	-
1318000903850000	Melbourne Regional Airport	-	-	-	-	-
1318000904000000	Port of Tampa, FL	6	1	-	-	7
1318000904010000	Port of St. Petersburg, FL	-	-	-	-	-
1318000904020000	Port of Manatee, FL	-	-	-	-	-
1318000904810000	Ft. Myers Regional Airport	-	-	-	-	-
1318000904830000	Sarasota Bradeton Airport	-	-	-	-	-
1320000900010000	Port of Mobile, AL	3	1	-	-	4
1320000900020000	Port of Gulfport, MS	-	-	-	-	-
1320000900030000	Port of Pascagoula, MS	-	-	-	-	-
1320000900040000	Port of Birmingham, AL	-	-	-	-	-
1320000900050000	Port of Huntsville, AL	-	-	-	-	-
1320000900060000	Port of New Orleans, LA	25	6	-	-	31
1320000900070000	Port of Memphis, TN	-	-	-	-	-
1320000900080000	Port of Baton Rouge, LA	-	-	-	-	-
1320000900090000	Port of Morgan City, LA	-	-	-	-	-
1320000900100000	Port of Little Rock, AK	-	-	-	-	-
1320000900110000	Port of Gramercy, LA	-	-	-	-	-
1320000900120000	Port of Greenville	-	-	-	-	-
1320000900130000	Port of Vicksburg, MS	-	-	-	-	-
1320000900140000	Port of Lake Charles, LA	-	-	-	-	-
1320000900150000	Port of Shreveport Bosier City, LA	-	-	-	-	-

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1320000900160000	Port of Nashville, TN	-	-	-	-	-
1320000900170000	Port of Chattanooga, TN	-	-	-	-	-
1320000900180000	Port of Knoxville, TN	-	-	-	-	-
1323000900010000	Port of Brownsville, TX	-	-	-	-	-
1323000900020000	Port of Del Rio, TX	-	-	-	-	-
1323000900030000	Port of Eagle Pass, TX	-	-	-	-	-
1323000900040000	Port of Laredo, TX	40	10	-	-	50
1323000900050000	Port of Hidalgo, TX	-	-	-	-	-
1323000900060000	Port of Roma, TX	-	-	-	-	-
1323000900070000	Port of Rio Grande City, TX	-	-	-	-	-
1323000900090000	Port of Progreso, TX	-	-	-	-	-
1323000902000000	Port of San Antonio,TX	-	-	-	-	-
1323000902010000	Port of Austin, TX	-	-	-	-	-
1324000900010000	Port of El Paso, TX	24	4	-	-	28
1324000900020000	Port of Presidio, TX	-	-	-	-	-
1324000900030000	Port of Fabens, TX	-	-	-	-	-
1324000900040000	Port of Columbus, NM	-	-	-	-	-
1324000900050000	Port of Albuquerque, NM	-	-	-	-	-
1324000900060000	Port of Santa Teresa, NM	-	-	-	-	-
1325000900011000	Port of San Ysidro, CA	1	0	-	-	1
1325000900012000	Port of Otay Mesa , CA	23	5	-	-	28
1325000900020000	Port of Tecate, CA	-	-	-	-	-
1325000900030000	Port of Calexico, CA	1	0	-	-	1
1325000900040000	Port of Andrade, CA	-	-	-	-	-
1326000902000000	Port of Douglas, AZ	-	-	-	-	-
1326000902010000	Port of Naco, AZ	-	-	-	-	-
1326000903000000	Port of Nogales, AZ	13	2	-	-	15

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1326000903010000	Port of Sasabe, AZ	-	-	-	-	-
1326000904000000	Port of Phoenix, AZ	5	1	-	-	6
1326000904010000	Port of Tucson, AZ	-	-	-	-	-
1326000905000000	Port of San Luis, AZ	-	-	-	-	-
1326000905010000	Port of Lukeville, AZ	-	-	-	-	-
1327000901100000	Port of Long Beach, CA	95	22	-	-	117
1327000901200000	Port of LAX	49	5	-	-	55
1328000902000000	Port of San Francisco, CA	59	13	-	-	72
1328000902010000	Port of Eureka, CA	-	-	-	-	-
1328000902020000	Port of Fresno, CA	-	-	-	-	-
1328000902030000	Port of Reno, NV	-	-	-	-	-
1328000902040000	Port of Salt Lake City, UT	-	-	-	-	-
1328000902050000	Port of San Jose, CA	-	-	-	-	-
1328000903000000	Port of Honolulu, HI	9	2	-	-	11
1328000903010000	Port of Hilo, HI	-	-	-	-	-
1328000903020000	Port of Kahului, HI	-	-	-	-	-
1329000900100000	Port of Denver, CO	3	1	-	-	4
1329000900018200	Natrona County International Airport	-	-	-	-	-
1329000900018300	Jefferson County Airport	-	-	-	-	-
1329000902000000	Port of Anchorage, AK	6	1	-	-	7
1329000902010000	Port of Juneau, AK	-	-	-	-	-
1329000902020000	Port of Ketchikan, AK	-	-	-	-	-
1329000902030000	Port of Skagway	-	-	-	-	-
1329000902040000	Port of Alcan, AK	-	-	-	-	-
1329000902050000	Port of Wrangell, AK	-	-	-	-	-
1329000902060000	Port of Dalton Cache, AK	-	-	-	-	-
1329000902070000	Port of Valdez, AK	-	-	-	-	-

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1329000902080000	Port of Fairbanks, AK	-	-	-	-	-
1329000902090000	Port of Sitka, AK	-	-	-	-	-
1329000902270000	Port of Kodiak, AK	-	-	-	-	-
1329000903000000	Port of Portland, OR	11	2	-	-	13
1329000903010000	Port of Astoria, OR	-	-	-	-	-
1329000903020000	Port of Newport, OR	-	-	-	-	-
1329000903030000	Port of Coos Bay, OR	-	-	-	-	-
1329000903040000	Port of Longview, WA	-	-	-	-	-
1329000903050000	Port of Boise, ID	-	-	-	-	-
1329000903820000	Rogue Valley-Medford User Fee Airport	-	-	-	-	-
1330000902000000	Port of Seattle, WA	28	6	-	-	34
1330000902010000	Port of Spokane, WA	-	-	-	-	-
1330000902820000	Grant County/Moses Lake User Fee Airport	-	-	-	-	-
1330000903000000	Port of Blaine, WA	19	3	-	-	22
1330000903010000	Port of Sumas, WA	-	-	-	-	-
1330000903020000	Port of Point Roberts, WA	-	-	-	-	-
1330000903030000	Port of Lynden, WA	-	-	-	-	-
1330000904000000	Port of Tacoma, WA	-	-	-	-	-
1330000904010000	Port of Aberdeen, WA	-	-	-	-	-
1330000904020000	Port of Bellinghham, WA	-	-	-	-	-
1330000904030000	Port of Everett, WA	-	-	-	-	-
1330000904040000	Port of Port Angeles, WA	-	-	-	-	-
1330000904050000	Port of Port Towsend, WA	-	-	-	-	-
1330000904060000	Port of Anacortes, WA	-	-	-	-	-
1330000904070000	Port of Friday Harbor, WA	-	-	-	-	-
1330000904090000	Port OF NEAH BAY, WA	-	-	-	-	-
1330000905000000	Port of Oroville, WA	-	-	-	-	-

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000905020000	Port of Danville, WA	-	-	-	-	-
1330000905030000	Port of Ferry, WA	-	-	-	-	-
1330000905050000	Port of Laurier, WA	-	-	-	-	-
1330000905060000	Port of Frontier, WA	-	-	-	-	-
1330000905070000	Port of Metaline Falls, WA	-	-	-	-	-
1330000906000000	Port of Duluth, MN	-	-	-	-	-
1330000906010000	Port of Ashland, WI	-	-	-	-	-
1330000906020000	Port of International Falls/Ranier, MN	-	-	-	-	-
1330000906030000	PortPortage, MN	-	-	-	-	-
1330000907000000	Port of Great Falls, MT	1	0	-	-	1
1330000907010000	Port of Raymond, MT	-	-	-	-	-
1330000907020000	Port of Eastport, ID	-	-	-	-	-
1330000907030000	Port of Butte, MT	-	-	-	-	-
1330000907040000	Port of Turner, MT	-	-	-	-	-
1330000907050000	Port of Porthill, ID	-	-	-	-	-
1330000907060000	Port of Scobey, MT	-	-	-	-	-
1330000907070000	Port of Sweetgrass, MT	-	-	-	-	-
1330000907080000	Port of Whitetail, MT	-	-	-	-	-
1330000907090000	Port of Piegan, MT	-	-	-	-	-
1330000907100000	Port of Opheim, MT	-	-	-	-	-
1330000907110000	Port of Roosevelle, MT	-	-	-	-	-
1330000907120000	Port of Morgan, MT	-	-	-	-	-
1330000907130000	Port of Whitlash, MT	-	-	-	-	-
1330000907140000	Port of Del Bonita, MT	-	-	-	-	-
1330000908000000	Port of Pembina, ND	9	2	-	-	11
1330000908020000	Port of Portal, ND	-	-	-	-	-
1330000908030000	Port of Neche, ND	-	-	-	-	-

Organization Code	Location Title	Import Specialists				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000908040000	Port of St. John, ND	-	-	-	-	-
1330000908050000	Port of Northgate, ND	-	-	-	-	-
1330000908060000	Port of Walhalla, ND	-	-	-	-	-
1330000908070000	Port of Hannah, ND	-	-	-	-	-
1330000908080000	Port of Sarles, ND	-	-	-	-	-
1330000908090000	Port of Ambrose, ND	-	-	-	-	-
1330000908100000	Port of Antler, ND	-	-	-	-	-
1330000908110000	Port of Sherwood, ND	-	-	-	-	-
1330000908120000	Port of Hansboro, ND	-	-	-	-	-
1330000908130000	Port of Maida, ND	-	-	-	-	-
1330000908140000	Port of Fortuna, ND	-	-	-	-	-
1330000908150000	Port of Westhope, ND	-	-	-	-	-
1330000908160000	Port of Noonan, ND	-	-	-	-	-
1330000908170000	Port of Carbury, ND	-	-	-	-	-
1330000908180000	Port of Dunseith, ND	-	-	-	-	-
1330000908190000	Port of Warroad, MN	-	-	-	-	-
1330000908200000	Port of Baudette, MN	-	-	-	-	-
1330000908220000	Port of Roseau, MN	-	-	-	-	-
1330000908810000	Hector User Fee Airport, Fargo	-	-	-	-	-
1358000900010000	Port of Detroit, MI	47	10	-	-	57
1338000900020000	Port of Port Huron, MI	-	-	-	-	-
1338000900030000	Port of Sault Sainte Marie, MI	-	-	-	-	-
1338000902000000	Port of Grand Rapids, MI	-	-	-	-	-
1338000902010000	Port of Battle Creek, MI	-	-	-	-	-
1338000902020000	Port of Saginaw/Bay City/Flint, MI	-	-	-	-	-
1338000902030000	Port of Muskegon, MI	-	-	-	-	-
1339000900020000	Port of Kansas City	2	1	-	-	3

		Import Specialists				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000900030000	Port of Cincinnati, OH/Lawrenceburg, IN	-	-	-	-	-
1339000900040000	Port of Columbus, OH	-	-	-	-	-
1339000900048200	Rickenbacker Airport	-	-	-	-	-
1339000900050000	Port of Dayton, OH	-	-	-	-	-
1339000900060000	Port of Toledo/Sandusky, OH	-	-	-	-	-
1339000900070000	Port of Louisville, KY	-	-	-	-	-
1339000900078400	Blue Grass Airport	-	-	-	-	-
1339000900080000	Port of Indianapolis, IN	-	-	-	-	-
1339000900088300	Baer Field Airport	-	-	-	-	-
1339000902000000	Port of Chicago, IL	44	9	-	-	53
1339000902010000	Port of Peoria, IL	-	-	-	-	-
1339000902020000	Port of Omaha, NE	-	-	-	-	-
1339000902030000	Port of Des Moines, IA	-	-	-	-	-
1339000902040000	Port of Davenport/Rock Island/Moline, IL	-	-	-	-	-
1339000902050000	Port of Rockford	-	-	-	-	-
1339000902810000	Waukegan Regional Airport	-	-	-	-	-
1339000902830000	Pal-Waukee Airport	-	-	-	-	-
1339000903000000	Port of Milwaukee, WI	3	1	-	-	4
1339000903020000	Port of Green Bay, WI	-	-	-	-	-
1339000903040000	PORT OF SHEBOYGAN, WI	-	-	-	-	-
1339000903050000	Port of Racine, WI	-	-	-	-	-
1339000904000000	Port of Cleveland, OH	32	5	-	-	37
1339000904010000	Port of Erie, PA	-	-	-	-	-
1339000904020000	Port of Owensboro, KY/Evansville, IN	-	-	-	-	-
1339000904030000	Port of Ashtabula/Conneaut, OH	-	-	-	-	-
1339000905000000	Port of St. Louis, MO	4	1	-	-	5
1339000905010000	PORT OF ST. JOSEPH, MO	-	-	-	-	-

Organization Code	Location Title	Import Specialists				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000905020000	Port of Wichita, KA	-	-	-	-	-
1339000905030000	Port of Springfield, MO	-	-	-	-	-
1339000906000000	Port of Minneapolis, MN	7	1	-	-	8
1339000906010000	Port of Sioux Falls, SD	-	-	-	-	-
1339000906810000	Rochester User Fee Airport	-	-	-	-	-
1339000990010000	Vancouver, Canada Preclearance	-	-	-	-	-
1339000990020000	Calgary, Canada Preclearance	-	-	-	-	-
1339000990030000	Edmonton, Canada Preclearance	-	-	-	-	-
1339000990040000	Montreal, Canada Preclearance	-	-	-	-	-
1339000990050000	Toronto, Canada Preclearance	-	-	-	-	-
1339000990080000	Winnepeg, Canada Preclearance	-	-	-	-	-
1339000990090000	Ottawa Canada Preclearance	-	-	-	-	-
1349000902000000	Port of San Juan, PR	15	3	-	-	18
1349000902020000	Port of Fajardo, PR	-	-	-	-	-
1349000902040000	Port of Huamaco, PR	-	-	-	-	-
1349000902050000	Port of Mayaguez, PR	-	-	-	-	-
1349000902060000	Port of Ponce, PR	-	-	-	-	-
1349000902070000	Port of Jobos, OR	-	-	-	-	-
1349000903000000	Port of Charlotte Amalie, VI	6	1	-	-	7
1349000903020000	PORT OF CORAL BAY VI	-	-	-	-	-
1349000903040000	PORT OF FREDERIKSTED VI	-	-	-	-	-
1352000900030000	Port of Port Everglades, FL	-	-	-	-	-
1352000900040000	Port of West Palm Beach, FL	-	-	-	-	-
1352000901010000	Miami Airport	34	5	-	-	39
1352000901020000	Miami Seaport	-	-	-	-	-
1352000990010000	Nassau, Bahamas	-	-	-	-	-
1352000990020000	Freeport, Bahamas	-	-	-	-	-

Organization Code	Location Title	Import Specialists				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1352000990030000	Kindley Field, Bermuda	-	-	-	-	-
1353000902000000	Port of Corpus Christi, TX	-	-	-	-	-
1353000903000000	Port of Dallas/Ft. Worth, TX	15	2	-	-	17
1353000903010000	Port of Amarillo, TX	-	-	-	-	-
1353000903020000	Port of Lubbock, TX	-	-	-	-	-
1353000903040000	Port of Oklahoma City, OK	-	-	-	-	-
1353000903050000	Port of Tulsa, OK	-	-	-	-	-
1353000903820000	Midland Airport	-	-	-	-	-
1353000904000000	Port of Houston, TX	17	4	-	-	21
1353000904010000	Port of Port Author, TX	-	-	-	-	-
1353000904030000	Port of Freeport, TX	-	-	-	-	-
1400000001040000	Regulatory Audit Division	-	-	-	-	-
0999099999999999	Mission Support	129	24	-	-	153

Appendix N – Optimal "All Other" Staffing Levels by Location (Preliminary)

Note: When calculated to the location level, the optimal additional Inspectors (5,080) and Agents (2,296) required for enforcement threat aggregate to a different number than when calculated globally (4,767 and 2,041, respectively). As a result, the "All Other" staffing level calculations also differ between the two types of enforcement threat calculations: 4,117 calculated at the local level versus 3,798 calculated at the global level. Again, to remain conservative in its estimates and to remain consistent with the other global calculations, Customs chose the smaller of the two numbers to include in its final staffing request.

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
	Total:	7,498	1,424	141	4,117	13,180
040000080901010	San Diego Aviation Branch	30	3	-	2	34
040000080901011	Riverside Aviation Unit	10	1	-	0	11
040000080901012	Sacramento Aviation Unit	2	0	-	-	2
040000080901012	Tucson Aviation Branch	43	5	-	4	52
040000080901012	Phoenix Aviation Unit	5	1	-	1	6
040000080901013	Albuquerque Aviation Branch	32	3	-	4	39
040000080901013	El Paso Aviation Unit	17	2	-	3	21
040000080901014	San Angelo Aviation Branch	40	4	-	3	47
040000080901014	San Antonio Unit	11	1	-	1	13
040000080901020	Surv Sup Ctr(Corpus Chris, TX)	89	5	-	-	93
040000080901020	PANAMA AVIATION UNIT	-	-	-	-	-
040000080901031	Jacksonville Aviation Branch	31	3	-	3	37
040000080901031	New York Aviation Unit	5	0	-	-	5
040000080901031	Tampa Aviation Unit	6	1	-	0	7
040000080901032	Houston Aviation Branch	31	3	-	1	35

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0400000809010321	Kansas City	1	0	-	-	1
0400000809010330	New Orleans Aviation Branch	27	3	-	6	36
0400000809010331	Pensacola Aviation Branch	6	1	-	0	7
0400000809010332	Cincinnati Aviation Branch	2	0	-	-	2
0400000809010340	Miami Aviation Branch	47	5	-	3	56
0400000809010350	Puerto Rico Aviation Branch	29	3	-	2	33
0400000809010351	Gateway - Puerto Rico Air Branch	5	0	-	-	5
0400000809010500	Domestic Air Interdictin Coordination Center (DAICC)	87	-	-	0	87
0400000809010510	Drug Interdiction Ops Center	9	-	-	-	9
0400601600000000	CUST ATTACHE, THE HAGUE NETH	-	-	-	-	-
0400601700000000	Senior Customs Rep - Interpol	-	-	-	-	-
0400601800000000	Customs Attache - Moscow	-	-	-	1	1
0400601900000000	Senior Customs Rep - Hong Kong,BCC	-	-	-	1	1
0400602100000000	Customs Attache - London, Eng	2	-	-	1	3
0400602200000000	Customs Attache - Pretoria, South Africa	1	-	-	1	2
0400602500000000	Customs Attache - Mexico City, Mex	1	-	-	1	2
0400602800000000	Customs Attache - Ottawa, Canada	1	-	-	2	3
0400603200000000	Customs Attache - Paris, France	1	-	-	2	3
0400603400000000	Customs Attache - Rome, Italy	1	-	-	3	4
0400603500000000	Customs Attache - Panama City	-	-	-	0	0
0400603600000000	CUSTOMS ADVISOR-PANAMA CITY	-	-	-	-	-
0400603700000000	Customs Attache - Tokyo, Japan	1	-	-	1	2
0400603800000000	Customs Attache - Bonn, Germany	1	-	-	2	3
0400603900000000	Customs Attache - Seoul, Korea	-	-	-	1	1
0400604000000000	Customs Attache - Bangkok, Thailand	1	-	-	1	2
0400604100000000	Customs Attache - Vienna, Austria	1	-	-	1	2
0400604300000000	CUSTOMS REP-MILAN, ITALY	-	-	-	-	-

Organization Code	Location Title	All Other				
			Required Additional			
		FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0400604400000000	Customs Attache - Singapore	1	-	-	1	2
0400604500000000	CUSTOMS REP-MERIDA, MEXICO	-	-	-	12	12
0400604600000000	Customs Rep - Monterrey, Mexico	-	-	-	1	1
0400604700000000	Customs Rep - Tijuana, Mexico	-	-	-	0	0
0400604800000000	Customs Attache - Montevideo, UR	-	-	-	1	1
0400604900000000	Customs Attache - Miami, FL	1	-	-	0	1
0400605100000000	Customs Attache - Caracas, Venezuela	-	-	-	1	1
0400605200000000	Customs Attache - Beijing, China	-	-	-	1	1
0400605300000000	Customs Attache - Bogota, Colombia	1	-	-	0	1
0400605400000000	Customs Rep - Frankfurt	-	-	-	0	0
0400680000000000	Customs Communications Center	8	-	-	-	8
0404000000000000	SAC Boston	19	-	-	18	38
0404000001000000	RAC Bangor, ME	1	-	-	3	3
0404000002000000	RAC New Haven, CT	1	-	-	3	4
0404000003000000	RAC Burlington, VT	2	-	-	3	5
0409000000000000	SAC Buffalo, NY	10	-	-	11	21
0409000001000000	RAC Rouses Point, NY	4	-	-	7	11
0410000000000000	SAC New York, NY	39	-	-	38	78
0410000001000000	DSAC JFK International Airport	8	-	-	35	43
0410000001010000	RAC Long Island	3	-	-	9	12
0410000002000000	DSAC Newark, NJ	13	-	-	35	47
0410000003000000	DSAC World Trade Center	20	-	-	-	20
0413000000000000	SAC Baltimore	9	-	-	16	25
0413000001000000	RAC Philadelphia, PA	15	-	-	23	38
0413000002000000	RAC Washington, DC	4	-	-	15	19
0417000000000000	SAC Atlanta	10	-	-	15	25
0417000001000000	RAC Charleston, SC	5	-	-	6	11

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
04170000002000000	RAC Charlotte, NC	2	-	-	8	10
04170000003000000	RAC Savannah, GA	1	-	-	4	5
04170000004000000	RAC Greenville, SC	3	-	-	4	7
04170000005000000	RAC Norfolk, VA	3	-	-	8	11
04170000006000000	RAC Wilmington, NC	4	-	-	5	9
04180000000000000	SAC Tampa, FL	27	-	-	35	62
04180000001000000	RAC Port Canaveral, FL	3	-	-	3	6
04180000002000000	RAC Ft. Myers, FL	5	-	-	9	14
04180000003000000	RAC Jacksonville, FL	3	-	-	8	11
04180000004000000	RAC Orlando, FL	5	-	-	9	15
04180000005000000	RAC Panama City, FL	2	-	-	3	5
04180000006000000	RAC Pensacola, FL	1	-	-	5	6
04180000007000000	RAC Tallahassee, FL	3	-	-	4	7
04180000008000000	RAC Sarasota, FL	1	-	-	4	5
04200000000000000	SAC New Orleans	44	-	-	30	74
04200000001000000	RAC Lafayette, LA	2	-	-	4	6
04200000002000000	RAC Baton Rouge, LA	1	-	-	3	4
04200000003000000	RAC Lake Charles	3	-	-	2	5
04200000004000000	RAC Shreveport, LA	1	-	-	2	3
04200000005000000	RAC Little Rock, AR	1	-	-	2	3
04200000006000000	RAC Houma, LA	2	-	-	4	5
04200000007000000	RAC Gulfport, MS	10	-	-	8	18
04200000008000000	RAC Mobile	9	-	-	13	21
04200000009000000	RAC Memphis	1	-	-	3	4
04200000010000000	RAC Gulf Shores, AL	2	-	-	3	5
04200000011000000	RAC Birmingham, AL	1	-	-	3	4
04200000012000000	RAC Nashville, TN	1	-	-	4	5

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0423000000000000	SAC San Antonio, TX	14	-	-	13	27
0423000001000000	RAC Brownsville, TX	7	-	-	21	28
0423000002000000	RAC San Angelo/Midland, TX	1	-	-	6	7
0423000003000000	RAC Mc Allen, TX	6	-	-	-	6
0423000004000000	RAC Laredo, TX	4	-	-	17	21
0423000005000000	RAC Falcon Dam, TX	-	-	-	4	4
0423000006000000	RAC Eagle Pass, TX	1	-	-	5	6
0423000007000000	RAC Del Rio, TX	2	-	-	5	7
0424000000000000	SAC El Paso, TX	21	-	-	39	60
0424000001000000	RAC Albuquerque, NM	3	-	-	6	9
0424000002000000	RAC Deming, NM	1	-	-	7	8
0424000003000000	RAC Las Cruces, NM	2	-	-	8	10
0424000004000000	RAC Alpine	-	-	-	3	3
0425000000000000	SAC San Diego	35	-	-	41	76
0425000001000000	RAC Oceanside, CA	1	-	-	4	5
0425000002000000	RAC Calexico, CA	5	-	-	19	24
0425000003000000	RAC San Ysidro, CA	8	-	-	38	46
0426000000000000	SAC Tucson	25	-	-	20	45
0426000001000000	RAC Phoenix, AZ	1	-	-	5	6
0426000002000000	RAC Douglas, AZ	1	-	-	10	11
0426000003000000	RAC Nogales, AZ	5	-	-	17	22
0426000004000000	RAC Sellis, AZ	13	-	-	9	22
0426000005000000	RAC Yuma, AZ	2	-	-	9	11
0427000000000000	SAC Los Angeles, CA	35	-	-	32	66
0427000001000000	RAC Los Angeles Intl Airport	4	-	-	10	14
0427000002000000	RAC Riverside, CA	2	-	-	8	9
0427000003000000	RAC Orange County, CA	1	-	-	4	5

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0427000004000000	RAC Oxnard, CA	1	-	-	4	5
0427000005000000	RAC Las Vegas, NV	3	-	-	4	7
0428000000000000	SAC San Francisco, CA	8	-	-	15	23
0428000001000000	RAC San Francisco Intl Airport	1	-	-	5	6
0428000002000000	RAC San Jose, CA	2	-	-	5	7
0428000003000000	RAC Sacramento, CA	4	-	-	5	9
0428000004000000	RAC Honolulu, HI	6	-	-	9	14
0428000005000000	RAC Salt Lake City	1	-	-	3	4
0429000000000000	SAC Denver	9	-	-	9	18
0429000001000000	RAC Portland, OR	3	-	-	7	10
0430000000000000	SAC Seattle	7	-	-	13	20
0430000001000000	RAC Seattle-Tacoma, WA	1	-	-	4	5
0430000002000000	RAC Blaine, WA	3	-	-	10	13
0430000003000000	RAC Great Falls, MT	2	-	-	4	6
0438000000000000	SAC Detroit	9	-	-	19	28
0439000000000000	SAC Chicago	15	-	-	21	36
0439000001000000	RAC Minneapolis, MN	4	-	-	8	12
0439000002000000	RAC Cleveland, OH	6	-	-	8	14
0439000003000000	RAC Cincinnati, OH	2	-	-	3	5
0439000004000000	RAC St. Louis, MO	1	-	-	3	4
0439000005000000	RAC Kansas City, MO	1	-	-	3	4
0439000006000000	RAC Indianapolis, IN	2	-	-	3	5
0449000000000000	SAC San Juan, PR	33	-	-	27	60
0449000001000000	RAC Fajardo, PR	4	-	-	3	8
0449000002000000	RAC Mayaguez, PR	3	-	-	6	9
0449000003000000	RAC Ponce, PR	7	-	-	3	10
0449000004000000	RAC St. Thomas, VI	6	-	-	2	9

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
0452000000000000	SAC Miami, FL	84	-	-	84	168
0452000001000000	RAC Ft. Lauderdale, FL	10	-	-	13	24
0452000002000000	RAC Ft. Pierce, FL	3	-	-	4	7
0452000003000000	RAC Key Largo, FL	4	-	-	5	9
0452000004000000	RAC Key West, FL	6	-	-	8	14
0452000005000000	RAC West Palm Beach, FL	5	-	-	7	12
0453000000000000	SAC Houston	37	-	-	41	78
0453000001000000	RAC Galveston, TX	5	-	-	6	11
0453000002000000	RAC Corpus Christi, TX	3	-	-	8	11
0453000003000000	RAC Dallas, TX	8	-	-	20	28
1304000900010000	Port of St. Albans, VT	17	1	-	0	17
1304000902000000	Port of Portland, ME	10	1	-	4	15
1304000902010000	Port of Jackman, ME	2	1	8	1	12
1304000902020000	Port of Bangor, ME	-	0	-	1	2
1304000902030000	Port of Bath, ME	-	-	-	-	-
1304000902040000	Port of Bar Harbor, ME	-	0	-	0	0
1304000902050000	Port of Rockland, ME	-	-	-	-	-
1304000902060000	Port of Portsmouth, NH	-	0	-	0	0
1304000903000000	Port of Calais, ME	1	1	-	2	4
1304000903010000	Port of Eastport, ME	-	0	-	1	2
1304000903020000	Port of Vanceboro, ME	1	0	1	1	3
1304000903030000	Port of Jonesport, ME	-	-	-	-	-
1304000904000000	Port of Houlton, ME	3	2	7	3	15
1304000904010000	Port of Van Buren, ME	-	1	-	2	2
1304000904020000	Port of Madawaska, ME	-	0	2	2	4
1304000904030000	Port of Fort Kent, ME	-	0	2	2	4
1304000905000000	Port of Highgate Springs/Alburg, VT	2	2	-	5	9

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
130400090501000 0	Port of Richford, VT	1	1	4	3	8
130400090502000 0	Port of Burlington, VT	-	0	-	1	1
130400090600000 0	Port of Derby Line, VT	1	2	-	5	7
130400090601000 0	Port of Norton-Beecher Falls, VT	1	1	3	3	8
130400090700000 0	Port of Boston, MA	60	14	-	16	90
130400090701000 0	Port of Springfield, MA	-	0	-	0	0
130400090702000 0	Port of Worcester, MA	-	0	-	0	0
130400090703000 0	Port of Gloucester, MA	-	0	-	0	0
130400090704000 0	Port of New Bedford, MA	-	0	-	0	0
130400090800000 0	Port of Hartford, CT	2	1	-	1	4
130400090801000 0	Port of Bridgeport, CT	1	0	-	1	2
130400090802000 0	Port of New Haven, CT	-	0	-	0	0
130400090900000 0	Port of Providence, RI	4	0	-	0	5
130400090901000 0	Port of Newport, RI	-	0	-	0	0
130900090001000 0	Port of Albany, NY	1	0	-	1	2
130900090200000 0	Port of Champlain-Rouses Point, NY	32	7	-	20	59
130900090201000 0	Port of Trout River/Chateaugay/Ft. Covington	1	1	6	4	11
130900090300000 0	Port of Ogdensburg, NY	4	2	-	11	18
130900090302000 0	Port of Cape Vincent, NY	-	-	-	-	-
130900090304000 0	Port of Clayton, NY	-	-	-	-	-
130900090400000 0	Port of Buffalo, NY	70	15	-	34	120
130900090404000 0	Port of Syracuse, NY	1	0	-	1	2
131000090100000 0	Port of New York-Newark	290	49	-	58	397
131000090200000 0	Port of JFK Airport	228	44	-	137	409
131300090003000 0	Port of Chester, PA / Wilmington, DE	2	0	-	1	4
131300090004000 0	Port of Pittsburgh, PA	3	1	-	3	7
131300090005000 0	Port of Washington, DC	17	4	-	19	40

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
13130009000600000	Port of Alexandria, VA	-	0	-	1	1
13130009020000000	Port of Baltimore, MD	39	7	-	7	53
13130009020200000	PORT OF CAMBRIDGE, MD	-	-	-	-	-
13130009020300000	PORT OF CRISFIELD MD	-	-	-	-	-
13130009030000000	Port of Harrisburg, PA	2	0	-	0	3
13130009030100000	Port of Wilkes Barre/Scranton, PA	1	0	-	0	1
13130009410000000	Port of Philadelphia, PA	39	10	-	13	62
13130009410082000	Atlantic City User Fee Airport	-	0	-	0	0
13130009410100000	Port of Lehigh Valley, PA	-	0	-	0	0
13170009000100000	Port of Charlotte, NC	15	2	-	6	24
13170009000200000	Port of Charleston, SC	23	5	-	3	31
13170009000300000	Port of Atlanta, GA	22	5	-	16	43
13170009020000000	Port of Norfolk, VA	23	3	-	1	27
13170009020100000	Port of Newport News, VA	-	0	-	0	0
13170009030000000	Port of Richmond-Petersburg, VA	1	0	-	0	2
13170009030100000	Port of Charleston, WV	1	0	-	0	1
13170009030200000	Port of Front Royal, VA	-	-	-	-	-
13170009040000000	Port of Wilmington, NC	4	0	-	1	5
13170009040100000	Port of Reidsville, NC	-	-	-	-	-
13170009040200000	Port of Beaufort-Morehead, NC	-	0	-	0	1
13170009050000000	Port of Durham, NC	-	1	-	1	2
13170009050100000	Port of Winston Salem, NC	1	0	-	0	1
13170009070000000	Port of Greenville-Spartanburg, SC	4	0	-	1	5
13170009070100000	Port of Georgetown, SC	-	0	-	-	0
13170009070200000	Port of Columbia, SC	-	0	-	0	0
13170009080000000	Port of Savannah, GA	23	2	-	2	27
13170009080100000	Port of Brunswick, GA	1	0	-	0	1

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1318000902000000	Port of Jacksonville, FL	10	3	-	3	15
1318000902010000	Port of Fernandina, FL	-	0	-	0	0
1318000902020000	Port of Panama City, FL	-	0	-	0	0
1318000902030000	Port of Pensacola, FL	1	0	-	-	1
1318000903000000	Port of Orlando, FL	4	3	-	10	17
1318000903010000	Port of Port Canaveral, FL	1	1	-	3	5
1318000903020000	Sanford Regional Airport	-	0	-	2	2
1318000903840000	Daytona Beach Regional Airport	-	0	-	0	0
1318000903850000	Melbourne Regional Airport	-	0	-	0	0
1318000904000000	Port of Tampa, FL	19	3	-	1	23
1318000904010000	Port of St. Petersburg, FL	-	0	-	0	1
1318000904020000	Port of Manatee, FL	-	0	-	0	0
1318000904810000	Ft. Myers Regional Airport	-	0	-	0	0
1318000904830000	Sarasota Bradeton Airport	-	0	-	0	0
1320000900010000	Port of Mobile, AL	15	2	-	1	18
1320000900020000	Port of Gulfport, MS	-	0	-	0	1
1320000900030000	Port of Pascagoula, MS	1	0	-	0	1
1320000900040000	Port of Birmingham, AL	1	0	-	0	2
1320000900050000	Port of Huntsville, AL	1	0	-	0	1
1320000900060000	Port of New Orleans, LA	55	7	-	10	72
1320000900070000	Port of Memphis, TN	9	1	-	3	13
1320000900080000	Port of Baton Rouge, LA	2	0	-	0	3
1320000900090000	Port of Morgan City, LA	1	0	-	0	1
1320000900100000	Port of Little Rock, AK	1	0	-	0	1
1320000900110000	Port of Gramercy, LA	-	0	-	0	0
1320000900120000	Port of Greenville	-	-	-	-	-
1320000900130000	Port of Vicksburg, MS	-	0	-	0	0

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1320000900140000	Port of Lake Charles, LA	-	0	-	0	1
1320000900150000	Port of Shreveport-Bosier City, LA	1	0	-	0	1
1320000900160000	Port of Nashville, TN	2	1	-	1	3
1320000900170000	Port of Chattanooga, TN	1	0	-	0	1
1320000900180000	Port of Knoxville, TN	-	0	-	0	0
1323000900010000	Port of Brownsville, TX	8	8	-	36	52
1323000900020000	Port of Del Rio, TX	3	2	-	14	19
1323000900030000	Port of Eagle Pass, TX	6	3	-	22	31
1323000900040000	Port of Laredo, TX	56	24	-	54	134
1323000900050000	Port of Hidalgo, TX	6	5	-	42	53
1323000900060000	Port of Roma, TX	1	1	-	10	13
1323000900070000	Port of Rio Grande City, TX	1	1	-	3	5
1323000900090000	Port of Progreso, TX	2	1	-	10	13
1323000902000000	Port of San Antonio, TX	2	1	-	2	5
1323000902010000	Port of Austin, TX	1	0	-	0	1
1324000900010000	Port of El Paso, TX	47	17	-	90	154
1324000900020000	Port of Presidio, TX	1	1	-	9	11
1324000900030000	Port of Fabens, TX	-	1	-	6	7
1324000900040000	Port of Columbus, NM	1	1	-	5	7
1324000900050000	Port of Albuquerque, NM	-	0	-	1	1
1324000900060000	Port of Santa Teresa, NM	1	1	-	5	7
1325000900110000	Port of San Ysidro, CA	43	9	-	102	154
1325000900120000	Port of Otay Mesa, CA	29	12	-	13	54
1325000900020000	Port of Tecate, CA	1	1	-	6	9
1325000900030000	Port of Calexico, CA	17	12	-	41	69
1325000900040000	Port of Andrade, CA	-	0	-	6	7
1326000902000000	Port of Douglas, AZ	5	2	-	18	24

		All Other				
			Required Additional			
Organization Code	Location Title	FY 1998 Base	Workload	Border Presence	Enforcement Threat	Total
1326000902010000	Port of Naco, AZ	1	1	-	4	5
1326000903000000	Port of Nogales, AZ	38	8	-	42	88
1326000903010000	Port of Sasabe, AZ	-	0	1	1	2
1326000904000000	Port of Phoenix, AZ	5	2	-	4	10
1326000904010000	Port of Tucson, AZ	1	1	-	2	3
1326000905000000	Port of San Luis, AZ	5	3	-	18	26
1326000905010000	Port of Lukeville, AZ	1	0	-	2	4
1327000901100000	Port of Long Beach, CA	125	24	-	12	161
1327000901200000	Port of LAX	71	16	-	92	178
1328000902000000	Port of San Francisco, CA	144	25	-	35	203
1328000902010000	Port of Eureka, CA	-	0	-	0	0
1328000902020000	Port of Fresno, CA	-	0	-	0	0
1328000902030000	Port of Reno, NV	-	0	-	0	0
1328000902040000	Port of Salt Lake City, UT	1	0	-	0	1
1328000902050000	Port of San Jose, CA	-	0	-	0	1
1328000903000000	Port of Honolulu, HI	50	8	-	24	82
1328000903010000	Port of Hilo, HI	-	0	-	1	1
1328000903020000	Port of Kahului, HI	-	0	-	0	0
1329000900010000	Port of Denver, CO	7	1	-	4	12
1329000900015200	Natrona County International Airport	-	0	-	0	0
1329000900018300	Jefferson Country Airport	-	-	-	0	0
1329000902000000	Port of Anchorage, AK	16	2	-	2	21
1329000902010000	Port of Juneau, AK	-	0	-	0	0
1329000902020000	Port of Ketchikan, AK	-	0	-	1	1
1329000902030000	Port of Skagway	-	0	1	1	2
1329000902040000	Port of Alcan, AK	-	0	-	1	2
1329000902050000	Port of Wrangell, AK	-	0	-	0	0

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1329000902060000	Port of Dalton Cache, AK	-	0	1	1	2
1329000902070000	Port of Valdez, AK	-	0	-	0	0
1329000902080000	Port of Fairbanks, AK	-	0	-	0	0
1329000902090000	Port of Sitka, AK	-	0	-	0	0
1329000902270000	Port of Kodiak, AK	-	-	-	-	-
1329000903000000	Port of Portland, OR	20	3	-	4	27
1329000903010000	Port of Astoria, OR	-	0	-	0	0
1329000903020000	Port of Newport, OR	-	0	-	0	0
1329000903030000	Port of Coos Bay, OR	-	0	-	0	0
1329000903040000	Port of Longview, WA	-	0	-	0	0
1329000903050000	Port of Boise, ID	-	0	-	0	0
1329000903820000	Rogue Valley-Medford User Fee Airport	-	0	-	0	0
1330000902000000	Port of Seattle, WA	53	10	-	18	81
1330000902010000	Port of Spokane, WA	-	0	-	0	1
1330000902820000	Grant County/Moses Lake User Fee Airport	-	0	-	0	0
1330000903000000	Port of Blaine, WA	26	5	-	19	50
1330000903010000	Port of Sumas, WA	2	1	-	4	7
1330000903020000	Port of Point Roberts, WA	-	0	2	0	2
1330000903030000	Port of Lynden, WA	1	0	-	2	3
1330000904000000	Port of Tacoma, WA	6	1	-	0	7
1330000904010000	Port of Aberdeen, WA	-	0	-	0	0
1330000904020000	Port of Bellinghham, WA	-	0	-	0	1
1330000904030000	Port of Everett, WA	-	0	-	0	0
1330000904040000	Port of Port Angeles, WA	-	0	-	2	2
1330000904050000	Port of Port Towsend, WA	-	0	-	0	0
1330000904060000	Port of Anacortes, WA	-	0	-	2	2
1330000904070000	Port of Friday Harbor, WA	-	0	-	1	1

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000904090000	Port Of NEAH BAY, WA	-	-	-	-	-
1330000905000000	Port of Oroville, WA	-	1	0	3	4
1330000905020000	Port of Danville, WA	-	0	1	1	2
1330000905030000	Port of Ferry, WA	-	0	2	0	2
1330000905050000	Port of Laurier, WA	-	0	1	1	2
1330000905060000	Port of Frontier, WA	-	0	1	1	2
1330000905070000	Port of Metaline Falls, WA	-	0	1	1	2
1330000906000000	Port of Duluth, MN	4	0	-	1	5
1330000906010000	Port of Ashland, WI	-	-	-	-	-
1330000906020000	Port of International Falls/Ranier, MN	9	3	-	3	15
1330000906030000	PortPortage, MN	2	1	-	2	5
1330000907000000	Port of Great Falls, MT	11	1	1	1	13
1330000907010000	Port of Raymond, MT	-	0	-	1	1
1330000907020000	Port of Eastport, ID	-	1	2	1	4
1330000907030000	Port of Butte, MT	-	0	-	0	0
1330000907040000	Port of Turner, MT	-	0	2	0	2
1330000907050000	Port of Porthill, ID	-	0	1	1	2
1330000907060000	Port of Scobey, MT	-	0	2	0	2
1330000907070000	Port of Sweetgrass, MT	2	1	-	2	5
1330000907080000	Port of Whitetail, MT	-	0	2	0	2
1330000907090000	Port of Piegan, MT	-	0	1	1	2
1330000907100000	Port of Opheim, MT	-	0	2	0	2
1330000907110000	Port of Roosevilla, MT	-	0	-	1	2
1330000907120000	Port of Morgan, MT	-	0	2	0	2
1330000907130000	Port of Whitlash, MT	-	0	2	0	2
1330000907140000	Port of Del Bonita, MT	-	0	2	0	2
1330000908000000	Port of Pembina, ND	24	6	-	6	36

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1330000908020000	Port of Portal, ND	3	0	-	1	4
1330000908030000	Port of Neche, ND	-	0	2	0	2
1330000908040000	Port of St. John, ND	-	0	2	0	2
1330000908050000	Port of Northgate, ND	-	0	2	0	2
1330000908060000	Port of Walhalla, ND	-	0	2	0	2
1330000908070000	Port of Hannah, ND	-	0	2	0	2
1330000908080000	Port of Sarles, ND	-	0	2	0	2
1330000908090000	Port of Ambrose, ND	-	0	2	0	2
1330000908100000	Port of Antler, ND	-	0	2	0	2
1330000908110000	Port of Sherwood, ND	-	0	2	0	2
1330000908120000	Port of Hansboro, ND	-	0	2	0	2
1330000908130000	Port of Maida, ND	-	0	2	0	2
1330000908140000	Port of Fortuna, ND	-	0	2	0	2
1330000908150000	Port of Westhope, ND	-	0	2	0	2
1330000908160000	Port of Noonan, ND	-	0	2	0	2
1330000908170000	Port of Carbury, ND	-	0	-	0	0
1330000908180000	Port of Dunseith, ND	2	0	0	1	4
1330000908190000	Port of Warroad, MN	-	0	0	1	2
1330000908200000	Port of Baudette, MN	-	0	-	2	2
1330000908220000	Port of Roseau, MN	-	0	1	1	2
1330000908810000	Hector User Fee Airport, Fargo	-	0	-	0	0
1338000900010000	Port of Detroit, MI	76	22	-	34	132
1338000900020000	Port of Port Huron, MI	10	6	-	4	21
1338000900030000	Port of Sault Sainte Marie, MI	2	2	-	3	6
1338000902000000	Port of Grand Rapids, MI	-	0	-	0	0
1338000902010000	Port of Battle Creek, MI	-	0	-	0	0
1338000902020000	Port of Saginaw/Bay City/Flint, MI	-	0	-	0	0

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1338000902030000	Port of Muskegon, MI	-	-	-	-	-
1339000900020000	Port of Kansas City	5	1	-	-	6
1339000900030000	Port of Cincinnati, OH/Lawrenceburg, IN	7	1	-	4	12
1339000900040000	Port of Columbus, OH	4	0	-	1	5
1339000900048200	Rickenbacker Airport	-	-	-	-	-
1339000900050000	Port of Dayton, OH	4	0	-	1	5
1339000900060000	Port of Toledo/Sandusky, OH	1	0	-	1	2
1339000900070000	Port of Louisville, KY	5	0	-	0	5
1339000900078400	Blue Grass Airport	-	0	-	0	0
1339000900080000	Port of Indianapolis, IN	3	0	-	1	4
1339000900088300	Baer Field Airport	-	0	-	0	0
1339000902000000	Port of Chicago, IL	92	18	-	28	137
1339000902010000	Port of Peoria, IL	-	0	-	0	0
1339000902020000	Port of Omaha, NE	1	0	-	0	1
1339000902030000	Port of Des Moines, IA	-	0	-	0	0
1339000902040000	Port of Davenport/Rock Island/Moline, IL	-	0	-	0	0
1339000902050000	Port of Rockford	-	0	-	0	0
1339000902810000	Waukegan Regional Airport	-	0	-	0	0
1339000902830000	Pal-Waukee Airport	-	-	-	0	0
1339000903000000	Port of Milwaukee, WI	7	1	-	0	8
1339000903020000	Port of Green Bay, WI	-	0	-	0	0
1339000903040000	PORT OF SHEBOYGAN, WI	-	-	-	-	-
1339000903050000	Port of Racine, WI	-	0	-	0	0
1339000904000000	Port of Cleveland, OH	34	4	-	3	41
1339000904010000	Port of Erie, PA	-	0	-	0	0
1339000904020000	Port of Owensboro, KY/Evansville, IN	-	0	-	-	0
1339000904030000	Port of Ashtabula/Conneaut, OH	-	0	-	0	0

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1339000905000000	Port of St. Louis, MO	12	2	-	4	18
1339000905010000	PORT OF ST. JOSEPH, MO	-	-	-	-	-
1339000905020000	Port of Wichita, KA	-	0	-	0	0
1339000905030000	Port of Springfield, MO	-	0	-	0	0
1339000906000000	Port of Minneapolis, MN	18	3	-	6	27
1339000906010000	Port of Sioux Falls, SD	-	0	-	0	0
1339000906810000	Rochester User Fee Airport	-	0	-	0	0
1339000990010000	Vancouver, Canada Preclearance	-	1	-	6	8
1339000990020000	Calgary, Canada Preclearance	-	1	-	4	4
1339000990030000	Edmonton, Canada Preclearance	-	0	-	2	2
1339000990040000	Montreal, Canada Preclearance	-	1	-	6	8
1339000990050000	Toronto, Canada Preclearance	-	2	-	11	13
1339000990080000	Winnepeg, Canada Preclearance	-	0	-	2	2
1339000990090000	Ottawa, Canada Preclearance	-	0	-	2	2
1349000902000000	Port of San Juan, PR	66	12	-	31	108
1349000902020000	Port of Fajardo, PR	2	0	-	1	3
1349000902040000	Port of Huamaco, PR	-	-	-	-	-
1349000902050000	Port of Mayaguez, PR	3	1	-	1	4
1349000902060000	Port of Ponce, PR	3	0	-	0	3
1349000902070000	Port of Jobos, OR	-	-	-	-	-
1349000903000000	Port of Charlotte Amalie, VI	18	4	-	9	30
1349000903020000	PORT OF CORAL BAY, VI	-	-	-	-	-
1349000903040000	PORT OF FREDERIKSTED VI	-	-	-	-	-
1352000900030000	Port of Port Everglades, FL	6	6	-	13	25
1352000900040000	Port of West Palm Beach, FL	1	2	-	5	7
1352000901010000	Miami Airport	102	22	-	127	252
1352000901020000	Miami Seaport	11	10	-	15	36

		All Other				
			Required Additional			
Organization Code	Location Title	FY1998 Base	Workload	Border Presence	Enforcement Threat	Total
1352000990010000	Nassau, Bahamas	3	1	-	7	12
1352000990020000	Freeport, Bahamas	1	1	-	3	5
1352000990030000	Kindley Field, Bermuda	1	1	-	3	4
1353000902000000	Port of Corpus Christi, TX	-	0	-	0	0
1353000903000000	Port of Dallas/Ft. Worth, TX	32	6	-	36	74
1353000903010000	Port of Amarillo, TX	-	0	-	0	0
1353000903020000	Port of Lubbock, TX	-	0	-	0	0
1353000903040000	Port of Oklahoma City, OK	1	0	-	0	1
1353000903050000	Port of Tulsa, OK	1	0	-	0	1
1353000903820000	Midland Airport	-	0	-	0	0
1353000904000000	Port of Houston, TX	59	15	-	25	99
1353000904010000	Port of Port Author, TX	1	0	-	0	1
1353000904030000	Port of Freeport, TX	-	0	-	-	0
1400000001040000	Regulatory Audit Division	343	388	-	-	731
9999999999999999	Mission Support	3,238	395	45	1,178	4,857

December 6, 2001 Hearing follow-up responses to Q&As posed to Dr. Stephen E. Flynn, Senior Fellow for National Security, Council on Foreign Relations

Q: 1.*a) What can be done to facilitate better communication and coordination between frontline federal agencies in securing our ports?*

A: A first step is to map out the responsibilities and activities of the many federal, state, and local entities whose statutory mandates directs them to oversee some aspect of the cargo, conveyances, and operators that moves into and out our nation's ports. Once this mapping exercise is complete, recommendations should be formulated about what activities could be consolidated, eliminated, or done somewhere else besides the port. This streamlining exercise would make a significant contribution to helping to sort out who is responsible for what and what may have fallen through the gap.

A second step is to ensure that the key agency players have the information-age tools to receive, effectively manage, mine, and share data in an easily accessible format. This data must be presented early enough to allow front line agencies to conduct risk assessments before people or goods arrive in the port. This will require addressing bureaucratic and legal issues that restrict information from being shared among agencies or only require that data be made available after-the-fact for audits.

A third step is to mandate there be a port security committee established for each port, chaired by the U.S. Coast Guard Captain of the Port. These committees would be charged with meeting regularly to review and discuss vulnerability studies, proposed security upgrades, and response plans. The Captain of the Port should be staffed with a full-time liaison person to plan and organize these meetings and to ensure agreed upon follow-up actions are completed.

b) Have recent initiatives made since September 11 to your knowledge enhanced communications?

A: There is now far greater appreciation by virtually all the key players that the status quo is unacceptable. The stepped up efforts on port and container security within the Office of Naval Intelligence to support the analytical work of the U.S. Customs and U.S. Coast Guard is a very positive development. Still, at the field level, to my knowledge, recent efforts have had minimal effect on improving communications among the frontline agents. We remain a long way off from informed, coordinated communications and risk management across the responsible government agency representatives operating within a seaport.

c) In addition to the front line agencies, how can intelligence gathering also be effectively incorporated into the inter agency coordination process? How can federal agencies better coordinate and communicate with state and local authorities as well as the frequently private operators of ports, to best secure ports?

A: Detecting a crime or potential terrorist act within a seaport can be significantly enhanced by obtaining and maintaining a clear picture of the legitimate operations taking place within that port. This cataloging and monitoring of "normal" activities makes it

possible to quickly identify something out of the ordinary that may signal dangerous or malicious activity. To the casual eye, a busy port might appear to be hopelessly chaotic, making the act of detecting and intercepting bad things like trying to find a needle in a haystack. In actuality, while a port is always in motion, most of the actors are familiar ones, performing largely repetitive activities. A criminal or terrorist might try to blend into that busy port, but he is likely to behave in ways different from legitimate actors. Accordingly, private sector actors can make a substantial contribution to security by working with front line agencies in educating them on how their normal operations work, and also in reporting aberrant activities that they observe. The public sector, in turn, must do a much better job at providing security briefs to appropriate private sector leaders so that they can be more cognizant of potential threats. The issue of providing security clearances to appropriate state and local port authorities must be addressed since they tend to provide primary oversight for security within seaports. The Business Anti Smuggling Coalition (BASC), which was created by the U.S. Customs Service to enlist manufactures and importers in deterring detecting, and intercepting illicit drugs is an excellent model for this kind of an approach. The Harbor Safety Committees organized by the Coast Guard Captain of the Ports in most of the nation's major ports provides a model for information sharing among the local, state, and federal public and private stakeholders involved in a port.

Q: 2. Please elaborate on some of the specific logistical steps that would need to be taken to push the border back. For instance:
a) How would we get foreign governments to cooperate in some of these tasks, especially ones that will cost money - like setting up sanitized areas of the ports, hiring officials to physically inspect, pay for costly new technology, etc. ?

A: First, it is important to highlight to our trading partners the direct relationship of port and transportation security to the sustainability of global commerce. In the absence of a system-wide approach to security, a catastrophic terrorism act that involved ships, cargo, or ports may lead to the shutting down of the entire system until the breech in security can be identified, and corrective actions can be agreed upon and put in place. In the interim, much of global trade would effectively grind to a halt. The economic costs associated with such an action are difficult to estimate, but certainly would be massive when compared to expenses associated with security measures like investments in greater physical security and inspection technologies within the port.

Second, the absence of security already is translating into rising costs, primarily as a result of the nearly exponential growth in cargo theft which is a multi-billion dollar global industry. These losses are reflected in rising insurance costs. Ports experiencing a high incidence of theft and crime have a difficult time attracting and maintaining business from carriers, importers, and manufacturers. In addition, the absence of adequate port security controls also facilitates arms and contraband smuggling, trade and revenue fraud, and violations of export controls. In short, even in the absence of a terrorist incident, virtually all civilized countries have an individual and collective interest in improving port security.

Third, security measures that mandate greater levels of transparency and accountability also are conducive to monitoring the movements of goods through a supply chain and the more efficient management of transportation assets. Thus, if done intelligently, security measures can be sound investments in their own right.

b) Will we need US Customs agents at all these ports of origin to inspect? And if so, how many and how much will a project like this cost?

A: In some locales, it might be possible to effectively deputize the host customs agents to do the screening for us if we agree to reciprocate on our end. But, in most instances, placing U.S. Customs officials overseas in common bilateral or multilateral international inspection zones to pre-screen goods coming to the United States would be desirable because such an approach would make it possible to collect information at the point of departure, allow transport-related intelligence to get into the security system sooner, and reduce the congestion caused by concentrating all inspections at the final destination. The bilateral inspection zones set up by French and British officials at both ends of the English Channel tunnel could serve as a model. Specific dollar figures and personnel numbers have not been projected.

c and d) How much will these steps cost and who should pay for it? Should individual ports have to pay? and under what legal authority will Customs agents or other American officials act extraterritorially?

A: Costs will be shared by both public and private sectors. In general the aim is to have the private sector agree to pay for security measures up front, but reward them for doing so by providing them with a reduced risk of disruption in the event of a heightened terrorist alert. Also, it is important that these costs be borne by all the relevant players within a supply chain, and not just the ports or the major shipping liners. Finally, because these are indeed measures which are vital to U.S. national security, it is appropriate that public revenues, tax breaks, or other incentives be provided to support these measures, both at home and abroad.

The charters for the front-line agencies should be reviewed and modified to support a greater emphasis on international operations. In addition, there will need to be a stepped-up effort within the Department of States to negotiate agreements with foreign governments to advance this approach. The precedent already exists for Customs and Immigration officials acting overseas in cooperation with foreign governments in Canada, Ireland, and Bermuda.

Q: 3. Since there are at this time no federal standards for port security, what are the first steps we should be taking to establish such standards for physical security at ports? Even though every port is operated differently and there is no one-size-fits-all answer what are some of the most fundamental security guidelines that should be mandated and regulated at the federal level? Please comment specifically on proposals for biometric and other types of identification cards, background checks on all people with access to ports and even the potential federalization of port security personnel.

A: Securing the critical infrastructure at ports is important. Federal guidelines can be applied to ports through existing authorities to the extent that they insure basic physical security measures are in place (from a gates, guards and lights perspective) and establish standards for validating personnel who need to access the port for business. There are many existing off-the-shelf biometric technologies and personnel information databases that can be tested and implemented quickly if the resources are made available to put these systems in place.

Q: 4. How can the "In Bond" process be made safer – without overly sacrificing efficiency – so that Customs officials can make the best possible decisions, with the fullest of information about which containers should be targeted for inspection ?

A: US Customs officials do not presently have the capacity to apply, with a sufficient level of confidence, a "counter-terrorism" risk management approach to targeting containers. The "In Bond" process will only be made safer when the US moves away from placing primary reliance on a system of controls at the borders that lie within US jurisdiction and towards point of origin controls, supported by controls developed within international supply chains and accompanied by a concentric series of checks built into the system at points of transshipment and points of arrival.

Q: 5. What can and should we be doing to safeguard our borders now, at least from the most serious biological, chemical, radiological and nuclear threats, as opposed to more medium term or longer term plans that will take months or years to implement? Is there anything that can or should be done to protect our ports?

A: Unfortunately there is no quick fix. The front line agencies tasked with port security and the system under which they operate is broken. That said, the government should continue providing more money and manpower to woefully underfunded and understaffed inspection agencies. Inspector presence at the border is necessary but not at all sufficient. Any amount of inspectors and inspection technology cannot hope to handle the overwhelming volume and velocity of people and goods. But additional x-ray and gamma ray scanning equipment will certainly make inspections less personnel intensive, disruptive, and destructive. At a minimum, every port should have cargo scanning equipment and the additional 5-6 personnel per unit to maintain and operate them.

Q: 6. Some experts have stated that to secure our ports, all we really need to do is enforce the regulations that are currently on the books and ensure that the funding is there for the Agencies to do their jobs properly. Is this an accurate criticism? Are there already adequate security plans for ports that are just not being followed, due to lack of funds or other reasons? Or is further legislation needed to heighten security?

A: Ports should never be seen as a first line of defense. At best they are a last line of defense. Port security problems will not be solved in the ports themselves, but must be addressed in the larger transportation networks that bring ships, cargo, and their crews into those ports. More funding is certainly necessary for agencies tasked with securing ports, but port security must be imbedded into a broader agenda. Most of the port

security plans developed since September 11 attack the most obvious, and easiest to solve problem. Still, none of these plans have received the necessary funding to implement them. There is some risk that an ad hoc basis but even these are inadequate and cannot be properly implemented.

Q: 7. How do and should we address the issue of "flags of convenience" and the registration of ships? How can we best monitor and ensure the reliability of international information which we're provided about who and what is on a ship? Does this pose a significant security vulnerability to our ports and if so what should we do to resolve this unique problem?

A: The proper place to address issues regarding flags of convenience is within the International Maritime Organization (IMO). The IMO has been forward leaning on working to establish security standards within the global maritime community. In the short term, the most effective way to create a reliable international transportation security regime is for the President to empower the Secretary of Transportation to work with his counterparts in foreign ports to establish international standards. Enlisting mega-ports, focusing on point of origin security measures, and embracing the use of new technologies all support the homeland security mission of enhancing the ability of front line agencies to detect and intercept global terrorist activity before it can arrive at US ports. This approach also precludes the need to impose draconian security measure within seaports that has the effect of imposing a self-embargo on the American economy.

F. Amanda DeBusk
655 Fifteenth Street, N.W., Suite 900
Washington, D.C. 20005
(202) 626-6080
FAX: (202) 628-0858

December 31, 2001

VIA FACSIMILE AND REGULAR MAIL

Ms. Darla Cassell
Chief Clerk
Committee on Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Ms. Cassell:

I am writing in response to the December 10, 2001 letter from Chairman Joseph I. Lieberman forwarding additional questions related to the December 6 hearing entitled "Weak Links: Assessing the Vulnerability of U.S. Ports and Whether the Government is Adequately Structured to Safeguard Them." I appreciate having the opportunity to testify at the hearing and respond to the Committee's questions. Below are the Committee's questions, followed by my answers. For many of the answers, I rely on the Report of the Interagency Commission on Crime and Security in U.S. Seaports (Aug. 2000) ("Seaports Commission Report"). I was a Commissioner on that commission in my capacity as the Commerce Department Assistant Secretary for Export Enforcement (1997-2001).

Q1. What can be done to facilitate better communication and coordination between the front-line federal agencies in securing our ports? In addition to the front-line agencies, how can intelligence gathering also be effectively incorporated into the inter-agency coordination process? How can federal agencies better coordinate and communicate with state and local authorities, as well as the frequently private operators of ports, to best secure ports?

A1. The best way to facilitate communication and coordination is to have projects that bring the agencies together for a common purpose. S. 1214, Section 104 (Dec. 20, 2001 engrossed in Senate) requires the Secretary of Transportation to establish local port security committees. The legislation does not specify membership on those committees. It that legislation becomes law, the Secretary of Transportation should reach out to the front-line federal agencies to ensure that all participate in the port vulnerability assessments and follow-up implementation.

Concerning intelligence-gathering, it will be important to have a representative from the intelligence community on the local port security committees. Some of the best intelligence is

developed from open source information; representatives of the port security committee can support the intelligence community and vice versa. As recommended by the Seaports Commission, the intelligence community should increase foreign intelligence collection efforts aimed at providing specific, actionable information about those international criminal activities affecting seaports that have been identified as national security threats to the United States (e.g., proliferation of weapons of mass destruction). Seaports Commission Report, page 155.

Federal agencies can better coordinate and communicate with state and local authorities and private operators through the port security committees. S. 1214, Section 104 specifies that the committees are to draw on existing committees and include representatives of federal, state and local government and port authorities, among others.

Q2. Since there are at this time no federal standards for port security, what are the first steps we should be taking to establish such standards for physical security at ports? Even though every port is operated differently, and there is no one-size-fits-all answer, what are some of the most fundamental security guidelines that should be mandated and regulated at a federal level? Please comment specifically on proposals for biometric and other types of identification cards, background checks on all people with access to ports, and even the potential federalization of port security personnel.

A2. Answers to these questions follow:

Federal Standards for Port Security. The Seaports Commission developed model port guidelines. It did so because:

> The Commission found many publications that promoted security and provided guidelines. Some were published by the federal government, some by private sector firms, and some by trade associations. However, there were no generally accepted standards or guidelines to assist seaports in improving security. Without standards or guidelines, seaports have no benchmark to use if they choose to make a concerted effort to improve security. They also have no basis to measure the effectiveness of existing security measures.

Seaports Commission Report, page 76. Therefore, the Commission established a baseline against which to compare existing seaport security in four basic categories: (1) physical security and access control, (2) passenger and crew security, (3) cargo security, and (4) military mobilization security. The Commission recognized that due to differences in the ports, there was no one-size-fits-all answer. Therefore, it identified basic minimum guidelines and enhanced guidelines. It developed criteria for each category.

The physical security and access control section includes detailed guidelines for standard operating procedures, perimeter fence line, parking, access points, lighting, buildings, security force management and enhanced measures for physical security and access control in periods of

heightened risk. Seaports Commission Report, Appendix F: Model Port. For example, the perimeter fence line section contains the following guidelines:

- Fence line is intact, taut, well-secured to upright supports anchored into the ground, topped with bared wire on outward facing angle irons, and stands at least 8 feet (2.5 meters) in height.

- Reinforcement of the fence line with a barrier (e.g., ditch or berm) is used to enclose wheeled operations involving containers on chassis or trucks loaded with consolidated cargoes overnight, to render certain parts of the fence line physically impassible for a trailer.

- Alarms are installed to complement the security of a reinforced fence line to form a system capable of monitoring many alarm zones from a central control room manned by terminal security personnel.

These detailed security guidelines form a solid basis for federal standards.

Biometric and other types of identification cards. The Seaports Commission considered how technology can be used to enhance security. The Commission discussed biometric technologies:

> A variety of biometric technologies for access control are already on the market or under commercial development. They can be used to control access to a physical area or to a particular item such as a computer or vehicle. The specific biometric could be a person's fingerprint, handprint, facial image, iris or retina image, voice, handwriting, or thermal image. Each biometric usually has an associated cost, benefit, and drawback that must be considered as a specific installation is planned. At present, the least costly biometric technologies employ facial image, single fingerprint, and either voice or signature recognition. Unfortunately, these inexpensive technologies also are subject to delay or defeat as a result of external factors such as lighting, cuts, dirt, background noise, or immature design. The most accurate and reliable technologies are the most expensive, possibly as much as 50 times the cost of the less expensive devices. As a result, each biometric technology should be individually tested on site.

Seaports Commission Report, Appendix E: Technology, page 222. Since the report is over a year old, it is likely that there have been advances in biometric technology that might overcome some of the drawbacks identified by the Seaports Commission.

Background checks. The Seaports Commission recommended as part of the model port guidelines that background checks be used as an enhanced measure for physical security and access control in periods of heightened risk. Specifically, in the model port guidelines, the guideline states:

- All individuals employed in the seaport who have access to restricted or secure areas have been subject to background and criminal record checks.

Seaports Commission Report, Appendix F: Model Port, page 240.

For individuals with access to cargo, the Seaports Commission recommended the following minimal model port guidelines:

- Prospective employees are required to provide background information about previous employment history, criminal records, and drug use.
- All prospective employees are fingerprinted as part of the application process, and criminal history records are performed on all prospective employees (to the extent permitted by law).
- Employees have "drug awareness" and "security education" programs in effect for all employees.
- Employees wear distinctive identification cards or badges that act as authorization for accessing restricted areas.

Seaports Commission Report, Appendix F: Model Port, page 242.

In addition, the Seaports Commission has a specific recommendation for making certain guidelines mandatory if the voluntary model port concept has not improved security within five years. It calls for the Transportation Department to address

- A private sector credentialing process that limits access to sensitive seaport areas. States, unions, port authorities, and/or port terminal operators should administer this process. The national security committee should also assess the desirability and feasibility of utilizing criminal background checks to assist in determining access to restricted or sensitive areas at the seaports, including the advisability of port-specific approaches.

Seaports Commission Report, Executive Summary, page xvi.

S. 1214, Section 106 would implement many of the Seaport Commission recommendations on background checks. It requires the Secretary of Transportation to prescribe regulations for employment investigations and restrictions for security-sensitive positions.

Concerning the federalization of seaport security personnel, in my view it would be better for the federal government to enact standards than to federalize personnel. The federal government does not operate the seaports.

Q3. What can and should we be doing to safeguard our borders now, at least from the most serious biological, chemical, radiological, and nuclear threats, as opposed to more medium-term or longer-term plans that will take months or years to implement? Is there anything that can or should be done immediately to protect our ports?

A3. Answers to the questions follow:

Enhancing security now. There are many steps that the Congress could take now to enhance security. The Congress could require all ports to meet the model port minimum guidelines established by the Seaports Commission.

S. 1214, Section 105 draws on many elements of the model port guidelines. It requires maritime facility security plans to be developed and submitted. Each plan is to include provisions for physical security, procedural security, a credentialing requirement to limit access to waterfront facilities, a credentialing requirement to limit access to controlled areas for security-sensitive information, restrictions on vehicular access, restrictions on firearms and other dangerous weapons, use of appropriately qualified security officers, evacuation plans, a process for assessment and evaluation of safety and security of port areas after an emergency, and any other information the Secretary requires. These plan elements are good ones. However, the Seaports Commission found that the ports lacked guidelines in these areas. Seaports Commission Report at 76.

Building on S. 1214, Section 105, Congress could make federal funding for seaport security improvements contingent on the adoption of model port guidelines and allow a phase-in period for implementation. If the Congress does not tie standards to funding, there may be a hodgepodge of local security measures that do not necessarily take into account the national threat.

If the Congress decides not to deal with the entire set of model port guidelines, it could concentrate on particular elements such as physical security. Better physical security would make it more difficult for terrorists to gain access to our ports. S. 1214, Section 111 identifies 6 security-related items that qualify for funding. If the Congress chose to act quickly on physical security measures, it could mandate that each port implement these basic physical security measures rather than let the individual ports decide whether to implement these measures.

Since basic security is lacking at so many ports, implementing basic physical security measures would be costly. The Congress could limit the requirements to the top 50 ports (representing 90 % of U.S. cargo by tons) and limit requirements to the minimum adequate security guidelines recommended by the Seaports Commission.

Another area in which the Congress could take quick action concerns firearms. There is an illogical disparity between airports and seaports: no nail clippers are allowed beyond security at airports; but firearms are allowed at seaports. The Seaports Commission's model port guidelines recommend that firearms be restricted in the seaports to law enforcement personnel

and other approved individuals. Seaports Commission Report, Appendix F: Model Port, page 238. This recommendation could be implemented immediately.

Technology. While developing the intelligence and security enhancements to reduce the biological, chemical, radiological, and nuclear threats will take time, we can immediately increase our deployment of existing technology for detecting these threats. Chemical, radiological and nuclear detection devices are available and could be deployed at seaports immediately. The Seaports Commission analyzed the various technologies available. Trace detectors can detect explosive residue on clothing hands, lunch boxes, door handles, steering wheel, car trunks and so forth. Document scanners can look for explosive traces on entry passes and ID documents. Radiation detectors can identify nuclear weapons or hazardous materials. X-ray and gamma-imaging systems can detect explosives and other contraband. Also available are explosive particle and vapor trace detectors, explosive detection wipes and sprays, portable contraband detection systems, including dielectrometers and magnetic resonance for explosives in liquid form, and ultrasonic and video scanners for liquid-filled drums and tanks. Seaports Commission Report, Appendix E: Technology, pages 221-236.

In the model port guidelines, the Seaports Commission recommended that the minimal low-cost implementation technology for a relatively small seaport with a low risk of criminal activity and not designated as a military mobilization ports would be as follows:

> Contraband detection technology would consist of one mobile 2- and 6-MeV X-ray system, three mobile or relocatable gamma-imaging systems, a model X-ray van, and a number of portable and handheld devices including particle and vapor trace detectors for drugs and explosives. Radiation sensors would be at vehicle and pedestrian gates but no other locations. Approximate cost would be $8 million.

Seaports Commission Report at Appendix F; Model Port, page 246. The Congress could provide funding so that each of the 50 major seaports could immediately meet these minimal requirements. Further technology investments could be made based on the completion of vulnerability assessments required in S. 1214, Section 103.

Q4. Some experts have stated that to secure our ports, all we really need to do is enforce the regulations that are currently on the books, and ensure that the funding is there for the Agencies to do their jobs properly. Is that an accurate criticism? Are there already adequate security plans for ports that are just not being followed, due to lack of funds or other reasons? Or is further legislation needed to heighten security?

A4. No, I do not believe that all we really need to do is enforce the regulations currently on the books and ensure that funding is there. The Seaports Commission identified a large number of areas where new legislation is needed. S. 1214 contains many excellent provisions that implement many of the Seaports Commission recommendations and that will enhance security if it becomes law.

If the Committee has further questions or needs clarifications, I would be pleased to provide any follow up that would be helpful. I appreciate the opportunity to provide these views.

Sincerely,

F. Amanda DeBusk

Additional Questions for the Record
Submitted by Senator Joseph I. Lieberman
"Weak Links: Assessing the Vulnerability of U.S. Ports and Whether the Government is Asequately Structured to Safeguard Them"
December 6, 2001

Mr. Rob Quartel
CEO/Chairman, FreightDesk Technologies

RESPONSE DATE: FEBRUARY 22, 2002

1. What can be done to facilitate better communication and coordination between the front-line federal agencies in securing our ports? Have recent initiatives, made since September 11, to your knowledge enhanced communications? In addition to the front-line agencies, how can intelligence gathering also be effectively incorporated into the inter-agency coordination process? How can federal agencies better coordinate and communicate with state and local authorities, as well as the frequently private operators of ports, to best secure ports?

ANSWER: Others are probably better able to articulate a response to this question that gets to the issue of communications among the various jurisdictions and authorities that intersect at the port; and which addresses not only the mechanical issues, but those which also derive from the various separations of power and constitutional protections for the general population. There is no question, however, from my conversations with port directors around the country, that there are significant communications problems not only between the various levels of law enforcement but between them and the port and its own layers of jurisdiction.

Irrespective of this, I would argue that the port of debarkation in the United States is really the last, rather than the first, line of defense. The fact of the matter is that the port is a potential target, not just a gateway. Therefore, much of the new law enforcement activity contemplated in this legislation strikes me as symbolic, rather than particularly useful -- not unlike that which occurs at our airports, in which the National Guard stand with guns to protect against the least likely of threats – a direct charge through the screening area (usually hundreds of yards from the gates). That is not to say that there aren't real threats at the port – certain types of vessels (cruise ships, LNG tankers, oil tankers, etc) are certainly amenable to illegal seizure, in which case they become weapons themselves. USCG escorts and riders and tighter port movement controls are an appropriate response to this possible threat. And, while protection of the perimeter and containers contained therein is certainly a desired action in that it might protect against theft or pilferage, these actions do little or nothing to protect against the threat of container-based mass destruction: Protecting a container that carries a

weapon of mass destruction that has arrived from overseas from tampering once it is in the container yard just keeps the weapon safe. Let me reiterate, however, that I support tightened port security both here and in overseas ports as a desirable (if excessive) part of supply chain integrity.

The most effective means of protecting the ports from the threat of a weapon of mass destruction is to prevent a container carrying such a weapon from ever arriving in or passing through a US port to any destination either here or abroad. I have spoken to some of the means of accomplishing this in my testimony.

The rules of policy engagement should be these:

1. **Every shipment and container carrying it has to be presumed to potentially be a weapon of mass destruction.**

2. **Every ship, train, truck, or airplane carrying containers in not just international but domestic trade should be considered to be a potential delivery vehicle for a weapon.**

3. **Every port, airport, railhead, or receiving/loading dock should be considered to be both a potential terrorist target and a gateway to other targets.**

4. **Therefore, as a matter of public policy, every shipment and every container should be inspected, either physically or electronically, or both prior to embarking on transportation for the continental US; and the maintenance of the chain of custody and the cargo's physical integrity throughout the transportation/logistics process should considered to be a matter of high importance. Inspection by whatever means should take place between the manufacturing process and engagement in the transportation movement.**

Essentially, I suggest that **every container in international trade should be profiled through a new USG-based algorithm that makes use of both commercial and law enforcement/national security data, prior to loading on a vessel destined for a United States port.** Profiling activities should include the capture of non-Customs data (transportation and financial data, for example) in a protected data base maintained either by the Department of Commerce or by the Department of Transportation; then combined with NGS data managed by a national security agency such as the Office of Naval Intelligence, FBI, and others; and analyzed against a variety of factors and circumstances as described in more detail below.

The core fact that makes profiling practicable is that every international trade transaction generates hundreds of data points, beginning with the very purchase itself, as evidenced by a purchase order. The task here is to: (1) Capture the

data elements generated from the commercial transaction and the transportation and handling process that would allow a government agency to take the appropriate steps to profile a cargo for the probability of its containing a terrorist weapon; and to (2) Partner that profiling process with a hierarchy of organizational, regulatory, and either or both passive and intrusive inspection and verification processes. The central premise of this proposal is that the commercial sector already generates the basic data necessary; and that it merely needs to be captured, rationalized, and combined with other sources and algorithms to produce a profile. This can be done with minimal intrusion into the commercial process. I would note that earlier, more systematic data reporting, embedded in the commercial infrastructure, would produce the ancillary benefit of making the intermodal logistics system even more productive by increasing visibility to the key players in a transaction.

The difficulty with physical inspections, port security plans, customs agents, and other US-generated processes and mandates is that they certainly may intrude on the territorial integrity of other countries. Nevertheless, some if not all of these things have to be done. The trick is to figure out which are really useful, and which are "feel good." Some of the former can be imposed through coercive means, while others will require the cooperation of international organizations and their membership. Unfortunately, the speed at which international – particularly maritime – organizations move is glacial.

Thus, it seems to me that the preferred (and certainly the quickest) solution is to enlist the aid – again, either by mandate or coercively – of the private sector, which runs the international intermodal logistics processes today.

2. Please elaborate on some of the specific logistical steps that would need to be taken to "push the borders back." For instance:

- **How would we get foreign governments to cooperate in some of these tasks, especially ones that will cost money – like setting up sanitized areas of the ports, hiring officials to physically inspect, pay for costly new technology, etc.? What about foreign nations that don't want to, or are unable to, cooperate?**

- **Will we need U.S. Customs agents at all these ports of origin to inspect? And if so, how many, and how much will a project like this cost?**

- **How much will these steps cost, and who should pay for it? Should individual ports have to pay?**

- **Under what legal authority will Customs agents or other American officials act extraterritorially?**

ANSWER: The basic premise here is that the intelligent use of selected commercial and USG intelligence data could produce a profiling process that minimized the requirement for physical inspections, customs inspectors, etc, thus defying the assumption underlying the question.

In such a profiling scheme, 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 would 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 (neutron scanning, motion detection, etc) the container, 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.

Thus, the answer to the question of whether or not we would need to place US Customs inspectors inside foreign ports of embarkation 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.

As noted earlier, the alternative may be to negotiate bilaterals in which US Customs agents were directly stationed in overseas ports; or in which certain foreign customs services were authorized to act on behalf of the USG (although this would foster some discord in that certain countries would be offended at being denied the opportunity to be deputized).

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 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 whether or not US tariff rules are complied with. The latter has little to do with ascertaining the former. 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.

Two major attributes of this approach are that it: (1) Taps into the existing commercial trade management process and leverages existing relationships into a new holistic structure; and, (2) 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 topic I will address later.

3. Since there are at this time no federal standards for port security, what are the first steps we should be taking to establish such standards for physical security at ports? Even though every port is operated differently, and there is no one-size-fits-all answer, what are some of the most fundamental security guidelines that should be mandated and regulated at a federal level? Please comment specifically on proposals for biometric and other types of identification cards, background checks on all people with access to ports, and even the potential federalization of port security personnel.

ANSWER: I am not an expert on the issue standards, processes, and procedures are the most effective at protecting the physical integrity of the port, nor do I have much more than an educated layman's knowledge of biometrics, etc. Nevertheless, I can offer a few thoughts here based on some 30 years in the public policy process and over 20 years working specifically in transportation and in international trade.

I would begin by issuing a caution on the issue of the "no one-size-fits-all answer:" There are too many ports in the United States and overseas to leave each to its own discretion as to what measures constitute adequate security. The USG should establish a clear standard of performance, provide both technical and financial assistance in implementing it in ports of entry through which international shipments are in the future allowed to flow; and audit or otherwise periodically test these ports and procedures to guarantee their continuous operating integrity.

The last part of the question links a number of contentious issues in a way that is not necessary. ID cards seem to be generally accepted to be a good idea in these workplaces, and it is one for which there are variety of sophisticated and potentially low cost solutions. The issues here are more political than

substantive, frankly. One unspoken belief is that too many individuals working in ports as longshoremen or in other manual labor jobs there have histories that would disqualify them under the normal circumstances of a "background check. And what exactly are the uses to which such an ID card would be put? Just to check in to a facility? To be used as a constant, visible identifier while in the port? Or – one use to which I believe employees would strenuously object but to which employers would be strongly drawn – would ID's be used or available for use as a means of monitoring productivity and other activities? This is in large part a political question that will certainly come back repeatedly to test the will of numerous public officials and their native constituencies.

I would, for a number of operating reasons, oppose the creation of a federalized security work force in the ports of the United States. First and most importantly, ports are commercial enterprises, even while operating under quasi-public utility rules. Some operate in tandem with airports, others with elected Boards, yet others with a mixture of public and private facilities. I doubt that anyone would seriously argue that a federalized security work force should be placed in a terminal built by, for, and operated to the advantage of a commercial carrier. On the other hand, there is no question that the existing federal presence in ports of entry – the USCG, FBI, Customs, DEA, and others – creates a morass of confusion and discontinuous authorities. One federal agency should be given the clear, consistent authority in each port (or airport) for the coordination and execution of federal mandates, as well as being designated the formal point of contact on port security issues for civilian and commercial port entities. As a side note, these issues and solutions apply equally to rail and truck loading points for US destinations, as well as to air cargo facilities. If terrorists are diverted by security measures from ships and ocean ports, then they will take the path of least resistance, eg, unguarded loading docks and lightly guarded border crossings. I doubt that the government has the funds to provide federalized security forces at all of these commercial and non-commercial points.

4. How can the "In Bond" process be made safer – without overly sacrificing efficiency – so that Customs officials can make the best possible decisions, with the fullest amount of information, about which containers they should be targeting for inspection?

ANSWER: The answer to this question in part depends on the purpose for which Customs might target a container for inspection. If the issue is to ensure compliance with Customs rules (essentially revenue capture), then I would suggest that some version of what Customs is already doing is appropriate.

If, on the other hand, the purpose of an inspection is to prevent terrorism, then I would return here to my principal recommendation, which is that the USG employ a shipment profiling process to make this determination prior to the loading of a shipment or container on a vessel bound for the United States. Combining this with a rigorous sealing program at the point at which a container is loaded, and

then maintaining the physical integrity of the cargo throughout the transportation process, could make the "In Bond" process the procedure of choice for Customs officials as it already is for much of the commercial sector. I urge the Committee to consider that there is a legitimate question here as to whether or not Customs should be inspecting ANYTHING in the continental United States for the purpose of preventing terrorist acts. Customs is fundamentally a revenue agency. Thus, to mix revenue compliance with counter-terrorism should and is likely to foster a very strong reaction and substantial argument and delay from the commercial sector (shippers, intermediaries, consignees, carriers, etc) from which the USG needs cooperation – even under a mandatory program. Revenue and border compliance are simply not the same thing as a counter-terrorism response. Treating the latter as equivalent to the former or the former as a subset of the latter will almost certainly undermine our efforts to prevent WMD's from entering the United States.

5. What can and should we be doing to safeguard our borders now, at least from the most serious biological, chemical, radiological, and nuclear threats, as opposed to more medium-term or longer-term plans that will take months or years to implement? Is there anything that can or should be done immediately to protect our ports?

ANSWER: There are several actions that can be taken now:

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 Commisson; 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 adopt and mandate 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 by the private sector seeking to obtain transportation and supply chain visibility and control. They have NOT been solved yet by the government.

6. Some experts have stated that to secure our ports, all we really need to do is enforce the regulations that are currently on the books, and ensure that the funding is there for the Agencies to do their jobs properly. Is that an accurate criticism? Are there already adequate security plans for ports that are just not being followed, due to lack of funds or other reasons? Or is further legislation needed to heighten security?

ANSWER: There is no doubt some truth to both sides of this question. My conclusion, however, is that until a profiling or physical inspection program is in place OVERSEAS, prior to a cargo moving to the United States – then none of the current or anticipated procedures at the port will be sufficient to prevent a security breach. The underlying predicate to this question is fatally flawed, as it ignores the clear fact that the port itself is a potential target. It is all too little, too late.

7. How do and should we address the issue of "flags of convenience" and the registration of ships? How can we best monitor and ensure the reliability of international information which we're provided about who and what is on a ship? Does this pose a significant security vulnerability to our ports, and if so, what should we do to resolve this unique problem?

ANSWER: The term "flags of convenience" is not one that is either used or recognized in the commercial process. It is a political term, nothing more, nothing less, utterly without relevance or meaning to manufacturers and international transportation players, completely devoid of connection to the way the international shipping process actually works. What it is intended to convey politically is a sinister plot in which unpatriotic American (and major foreign) ship operators immorally move registration of their ships from countries like the United States with "good" ship operating and tax rules to countries with "bad" ones. The fact of the matter, however, is that with few exceptions these are business decisions, largely amoral, and they are taken for reasons that have nothing at all to do with either national fervor or a desire to cheat tax collectors. Because they are amoral, the logic suggests that, in fact, the "bad" rules are actually the ones – like those mandated by the US -- from which ship operators flee. The United States has passed numerous tax and operating rules that lie well outside of what is considered commonly accepted maritime business practice in the rest of the world, civilized or otherwise – in the process destroying its own fleet. That, however, is the topic for a book, not this particular hearing.

In the real world, ships are governed by a common set of international standards for ship construction, ship maintenance and operating procedures, and for labor practices. Whether we agree with them or not is irrelevant to the actual operating integrity of the companies that own these ships. As a practical matter, perhaps as much as 80 percent of all cargoes -- including all those bound for the United States in ocean containers -- are carried on no more than 10 well-respected, major, internationally operated (non-US) ocean carriers. Comparable numbers

exist for international air cargo. Domestic (inland rail and truck) companies operate under local rules, however, so are much more heterogeneous in size, capabilities, integrity, etc.

Without going into detail, the trade process itself is also highly regulated at the international level, with huge variations among countries in terms of customs rules and procedures, reporting requirements, etc. Anecdotally, many attribute the "toughest" customs rules to Brazil, and many would place the US at the high center of the pack. Rules and procedures varyingly affect how goods are documented into and out of a container, placed onto transportation, how insurance is to be applied, and so forth. While many foreign concerns use an International Bill of Lading owned by the International Freight Forwarders Association (FIATA), Americans typically do not – but its use could be mandated, at least in the short term, for purposes of international consistency. Certain materials are highly regulated by common convention and agreement, hazardous materials, and that also provides additional data integrity.

The bottom line is that the process spews data, from the moment a purchase order is placed, to the creation of a shipment, to the transportation booking, delivery, and actual placement on a shelf or use in the manufacturing process. At each step of the way, data is generally supposed to be synchronized for fulfillment and chain of custody purposes – with widely varying degrees of success. Of the 200 or so data elements that might be attributable to a single shipment in international trade, some 80 percent of that data is said to be entered and reentered multiple – often as many as 10 – times. It is typically a highly labor intensive process, whether it involves the ship or the train, the container, or just moving it into or out of a warehouse. And, while transportation data is largely moved by EDS, much of it comes in the form of faxes, email, or even voice messaging – and now, over the web. These are the types of issues that have confronted the transportation software industry and its clients seeking logistics controls and visibility for well over two decades, and which are just now being solved in the private marketplace.

Data on who owns ships, how they were financed, etc is both publicly available and privately withheld, some in offshore entities. There are perhaps some actions we need to take there, particularly on financial ownership issues, but otherwise most of the relevant data is easily available and can be connected to current manifest filings and crew lists.

The bottom line is that the country in which a ship is registered is largely irrelevant as long as ships and their owners and crews comply with accepted international standards. We really have no choice in this matter, anyway, as the United States no longer has an international deepwater container fleet – even one ship, in fact. However, because we are 20 percent of all world trade on any given day, we have immense leverage in the way the trade process is executed, not only with the individual companies involved, but with the governments and countries that benefit from that trade. What is most important is that we use the knowledge already embedded in the commercial sector to ascertain and improve the reliability of data and its use.

Additional Questions for the Record
Submitted by Senator Joseph I. Lieberman
"Weak Links: Assessing the Vulnerability of U.S. Ports and
Whether the Government is Adequately Structured to Safeguard Them"
December 6, 2001

Response by: R.M. Larrabee
Director, Port Commerce Department
Port Authority of New York and New Jersey

1a. **What can be done to facilitative better communication and coordination between the frontline federal agencies in securing our ports?** There has been an ongoing debate in Washington as to whose responsibility Port Security is. A key to better communication and coordination is in the answer to the question: "who is in charge? In terms of coordination at the top, the creation of the Office of Homeland Security is the White House and the appointment of Governor Tom Ridge was an important first step. That set the right tone that cooperation and coordination was mandated by the President. The administration must be vigilant to make sure that the departments and agencies from the Cabinet level down are cooperating. Congress establishing the transportation security post at DOT was the next important step with the clear message that security in ports and other sectors was a priority. Coordination among DOT agencies is in the Secretary's office as it should be. In my mind there is no doubt that the Coast Guard, whose primary mission relates to port safety and security, should have the lead in the marine sector in DOT and in implementing policy and incident response at the local level. We have seen evidence that there is good cooperation between the Coast Guard and the Maritime Administration, the principal marine oriented entities within DOT. In the field, the Coast Guard has good working relationships, the most knowledge of ports and terminals, and the unique military and civil law enforcement authority to take the lead in facilitating better communication and coordination related to port security. Note that the service has limited jurisdiction as you move further inland from the shore. As such Congress should consider whether the Coast Guard's area of responsibility should be expanded to include the landside portion of ports and terminals.

1b. **Have recent initiatives, made since September 11, to your knowledge enhanced communication?** Since September 11, there has been an unprecedented level of cooperation between the state, local and federal agencies. There is a greater understanding now about what each agencies roles and responsibilities are. At the same time though, it has heightened the confusion over "who is in charge?" and how multiple agencies interact and co-exist. We have also discovered that the same tasks are often being done by different agencies. We need to better plan/coordinate so that a broader scope of issues is being addressed rather the same thing 2 or 3 times by different agencies.

1c. **In addition to the frontline agencies, how can intelligence gathering also be effectively incorporated into the inter-agency coordination process?** Low-level intelligence has been shared on an increased level but that are no guidelines that indicate that agencies must share information with each other and outline the extent of the sharing. We have experienced instances since September 11th when agencies have shared critical information with us in the morning but when that staff is relieved in the afternoon, we can't get any information out of them. There is not a consistent understanding or policy on information sharing.

1d. **How can federal agencies better coordinate and communicate with state and local authorities, as well as the frequently private operators of ports, to best secure ports?** Through the establishment of Port Security Committees and the issuance of security clearances when needed (see #2).

2. **You mentioned at the hearing that you have not yet been given a security clearance at the Port Authority, despite your former position in the Coast Guard. What concrete steps can be taken to better facilitate the flow of information between the government and the Port Authority officials to strengthen security?** The federal agencies do not generally view Port Authority personnel, and certainly not personnel at private terminals, as part of the solution and therefore not capable of holding security clearances. That belief needs to be changed from the top down. In today's environment, the processing of security clearances for people who "need to know" needs to be expedited. Those with security clearances can be limited to a very few, perhaps a port authority and a law enforcement official in each port, and therefore keep the volume of clearances low. We are hearing now that it could take over a year for a new security clearance application to be processed. In additional, there must be a way to re-activate a previous clearance at the same level or below, without going through the entire process. Possibly a simplified update with a 10-year time limit on reactivation. This would ease the process as well as save the government a great deal of money.

3. **You also mentioned that the International Maritime Organization could play an important role in heightening security globally. What specific steps would you recommend to engage international organizations, either in dialogue or through international treaties, to ensure greater port security?** The IMO has a long and successful history of establishing international standards regarding safety of the maritime industry. The international aspect of port security must be brought to the attention of the IMO. The Commandant of the Coast Guard, Admiral Loy, addressed the IMO in December 2001, and got them to agree to establish a Port Security Working Group to address this issue. The IMO has the ability to effect the changes that are necessary to make changes in the way maritime security is addressed world-wide, but it traditionally taken the IMO many years to do that. Nations throughout the world have a vested interest in port security and together should influence the IMO to take action and proceed expeditiously. The determination on the part of member nation's top leaders that this is a

priority might help speed the IMO in its deliberations. This process should be monitored very closely particularly as it relates to the security of containers entering our nation's ports.

4a. **How would we get foreign governments to cooperate in some of these tasks, especially ones that will cost money – like setting up sanitized areas of the port, hiring officials to physically inspect, pay for costly new technology, etc? What about foreign nations that don't want to, or are unable to cooperate?** The president has made it eminently clear to the leaders of nations what the United States expects of them in the global fight against terrorism. Cooperation in making international trade a secure environment should be added to those expectations. Another way is through the successful development of public/private partnerships. These partnerships must include four key elements: the program must be constructive, not punitive; there must be international standards to measure compliance; the sanctions must be immediate and strong; and there is systematic, overseas monitoring. US Customs already has established partnerships in three different contraband interdiction programs, which can be used as the basis for a WMD interdiction program. Initiatives overseas by Customs, etc are an absolutely essential element in US port security policy because it is impossible to inspect every container arriving at U.S. ports.

4b. **Will we need U.S. Customs agents at all of these ports of origin to inspect? And if so, how many, and how much will a project like this cost?** There is a valid analogy between Customs experience with passenger pre-clearance and the proposal for cargo pre-clearance. In the existing programs, sovereign nations limit the enforcement of U.S. laws within their borders and refuse to allow U.S. Customs to collect data on their citizens. Rather than performing physical inspections overseas, it may be better to focus on certifying the integrity of a specific business process and manage the risk by knowing all the players in the chain of custody. A parallel program is the Department of Agriculture's certification of overseas food processing plants. A need may also arise to develop Special Operations teams that can immediately respond to seaports to augment existing staff resources as needed.

5. **Since there are at this time no federal standards for port security, what are the first steps we should be taking to establish such standards for physical security at ports? Even though every port is operated differently and there is no one size fits all answer, what are some of the most fundamental security guidelines that should be mandated and regulated at a federal level? Please comment specifically on proposals for biometrics and other types of identification cards, background checks on all people with access to ports, and even the potential federalization of port security personnel.** We are not in agreement that across the board federal standards for port security are required and believe that industry and security objectives would be better served by guidelines rather than standards. Standards are appropriate in some

instances and guidelines should be used to complete the federal expectations or requirements for ports. For example, every terminal has a dock and a gate; therefore some standard would be possible to take security to a certain level.

Ports are too unique to be held to strict standards. Rather, in conjunction with the Coast Guard Captain of the Port and results of the vulnerability assessment, individual security plans should be developed based on guidelines and individual circumstances. The guidelines should be generic and include things such as perimeter and procedural security, vehicular and personnel access, identification cards, and emergency response. The thought of issuing ID cards to all port workers is a monumental task and must be carefully though out. Some of the problems include: who is authorized to perform the background checks and issue the cards, who will pay for this, especially when workers will have access to multiple locations, interoperability of cards not only within a port but nationwide as truckers, longshoremen and even ship service provides will need access to numerous ports without having to carry individual cards for each one. At least a partial solution is a national transportation ID in as much as there is a national commercial drivers license. Finally, I don't believe that there is any need to "federalize" port security personnel especially they are going to be required to go through a background and credentialing process.

6. How can the "In-Bond" process be made safer – without overly sacrificing efficiency – sop that Customs officials can make the best possible decisions, with the fullest amount of information, about which containers they should be targeting for inspection?

The In-Bond process allows for the transfer of imported merchandise, either within a specific port of entry or between two ports of entry without the opportunity for government inspection. The key to managing the risk associated with this process is to streamline the inventory control process. We should focus on using the unique Bill of Lading number as the control number. If valid manifest data is used as the first layer to run against artificial intelligence systems, there should be no difference between port of entry cargo and in-bond cargo. Each port needs to develop an intercept plan that can be carried out 24x7. In addition, one need that must be satisfied is the identification of a Notified Party so that the targeting inspector can get additional information at the POE prior to the cargo moving on.

7. What can and should we be doing to safeguard our borders now, at least from the most serious biological, chemical, radiological and nuclear threats, as opposed to more medium-term or longer-term plans that will take months or years to implement? Is there anything can or should be done immediately to protect our borders? Establishment of more and use of domestic Coast Guard Port Security Units. We should also expand and rapidly implement the concept of using licensed Merchant Mariners as Sea Marshals and take advantage of the Coast Guards 6-week Boarding

Officer School. Further consideration might be given to requiring graduates of the US Merchant Marine Academy (Kings Point) to serve a period of time after graduation as Sea Marshals. Right now their obligation after graduation is to sail on a US merchant ship for a period of time or to work ashore for 4 years in a qualifying commercial maritime industry job. There is no pure requirement for graduates to serve the federal government in return for their education.

8. Some experts have stated that to secure our ports, all we really need to do is to enforce the regulations that are currently on the books, and ensure that the funding is there for the Agencies to do their jobs properly. Is that an accurate criticism? No, that is not all that needs to be done. The Coast Guard, for example, does have broad authority and given far greater resources and regulatory initiative USCG could put in place a more secure system. However, the objective of the Senate-passed bill (S 1214) and, ultimately, the enactment by Congress of maritime security legislation, is to create a much more effective security framework that is beyond the ability of current law and regulation. Congress must set the tone by mandating action, establishing the respective roles of Federal, State and local agencies, and providing the necessary resources. The executive branch must follow through, domestically and internationally, to put the framework in place. Having said that, it is essential that I underscore that one of the most critical elements of heightening port security is ensuring adequate funding and resources for the various federal agencies. Personnel and resources that were deployed to the Port of NY & NJ in the immediate aftermath of September 11th, were not sustainable and were released from service in our area without there being any change in the threat or vulnerability of our region. In addition, the primary missions of these agencies were temporarily suspended while they were redeployed to port security activities.

Are there already adequate security plans for ports that are just not being followed, due to lack of funds or other reasons or is further legislation needed to heighten security? Although, every marine terminal has a security plan, they are not currently required to be vetted by the Coast Guard. If adequate Coast Guard resources are available it is advisable for the Coast Guard to review all plans. More important however is the contents of individual security plans must be combined to form a consolidated security/terrorism annex to the Area Contingency Plan.

9. How do and should we address the issue of "flags of convenience" and the registration of ships? How can we best monitor and ensure the reliability of international information that we are provided about who and what is on a ship? Does this pose a significant security vulnerability to our ports, and if so, what should be done to resolve this unique problem? Large portions of the international maritime community have a Port State Control system in place to accurately monitor vessels flying "flags of convenience" and increase the emphasis on the examination of foreign vessels. Although the current emphasis is primarily driven by requirements to ensure compliance with pollution prevention and navigation safety regulations, potential crime and terrorism precursors are being stressed. The new Coast Guard 96-hour rule for making pre-notification of a vessels arrival, along with the additional data elements that are now being required is a good step to review who and what is purported to be on the ship, in a more timely manner. We cannot place too much emphasis though on this pre-screening just days before a vessel hits our shores. The information is only as good as the information that honest and conscientious shippers, steamship lines and countries want to share with us. Public-private partnerships with clear information on the chain of custody are critical, as a terrorist is not going to identify a potentially dangerous cargo or crew member as one that our federal agencies is targeting.

January 3, 2002

Honorable Joseph I. Lieberman
Chairman,
Committee on Governmental Affairs
United States Senate
Washington, DC 20610-6250

Dear Chairman Lieberman:

Thank you for allowing me to address your committee on the important issue entitled "Weak Links: Assessing the Vulnerability of U.S. Ports and Whether the Government is Adequately Structured to Safeguard Them". I believe that the security of our ports is in question and I am committed to doing whatever it will take to make my port, my family, my community and our nation safe. I have addressed the additional questions from the hearing below:

1. Since September 11th, many of our nation's priorities have shifted. A U.S. Customs Service internal study performed last year found that approximately 14,000 additional people were needed to complete its mission, and this was prior to 9-11.

Mr. Acosta, you are a Customs Inspector at the Port of New Orleans. However, I noted from your testimony that you also have a temporary duty assignment which has already required you to man Port Huron, along the northern border, once already this year, and that you are likely to return to Port Huron sometime in the coming months. Are temporary duty assignments a regular occurrence? What weaknesses and strains on the system does shuttling inspectors from port to port produce?

I have completed one temporary duty assignment, immediately following September 11th., to the northern border port of Port Huron and I will begin a second assignment there on January 8th, of this month. Both of my assignments were voluntary. Since September 11th such assignments from the port of New Orleans have been a regular occurrence. In fact, the Gulf CMC, the Custom's management area consisting of the states of Louisiana, Tennessee, Alabama, Mississippi and Arkansas has contributed 12 inspectors/canine officers per month to the effort at Detroit/Port Huron since September 11th. The majority of our personnel have been volunteers, however, some have been ordered to travel in order to meet our commitment. Customs has a history of responding to areas of temporary need (Olympics, national enforcement efforts, etc.) with TDY personnel. Obviously it is a system that meets one need (the need for increased manpower on the northern border) but produces shortages in the donor ports which should also be on a heightened alert. There is no replacement for specific experience and training in a given area. Customs has reduced functions and manpower to meet funding shortages for some years and I believe that nowhere is this more visible than at the nation's seaports.

2. Some people have suggested mandating background checks for all personnel with access to vessels and sterilized areas of ports, in addition to making one agency responsible for the issuance of all port-related identification cards. Do you believe this is a good idea?

My experience is that we get what we pay for. For example, we hold federal employees to a high standard of accountability, and to this end we perform an extensive background investigation before we hire them. Many of these employees are then subjected to periodic background checks and random drug screening. As a result federal employees represent one of the most reliable, stable and loyal workforces in the world. Thirty or more years ago the U.S. Customs Service was a very visible and accountable agency at our nation's ports. Customs inspectors were the part of our service referred to as I & C (inspection and control). Sadly, budget cuts, budget shortfalls and a loss of focus on seaports have cost us most of the control we once enjoyed. A search of the Federal Regulations which Customs operates under will show many procedures which were in place to insure a level of security at our nation's ports. Most of these have been abandoned or circumvented due to the reality of limited resources and manpower.

I believe that one agency which would be responsible for seaport security issues would be a good idea. Historically the Customs Service was that agency. Given the resource and budget problems that it is faced with today it could not accomplish this task without assistance from Congress in the help of a realistic budget which would allow it to operate as prescribed by the federal regulations which govern it.

Sincerely,

Argent Acosta

Argent Acosta

RESPONSES FROM MICHAEL D. LADEN
TO QUESTIONS FOR THE RECORD

"Weak Links: Assessing the Vulnerability of U.S. Ports and Whether the Government is Adequately Structured to Safeguard Them?

December 6, 2001

Question: What lessons were learned from the creation and implementation of BASC which can apply to our current efforts to secure our ports and intermodal transportation system from acts of terrorism?

The creation of the Business Anti-Smuggling Coalition (BASC) in 1995 represented the first tangible effort, on the part of the private sector and the Customs Service, to form a meaningful partnership to combat the flow of illicit narcotics. Certainly, one of the most important things learned from this exercise was, that the private sector and the Customs Service, through partnership, could build an effective system to deter commercial contamination.

The BASC Program allows the U.S. Customs Service to essentially separate the 'known shipper,' from the 'unknown shipper.' This is vital in assessing and managing risk, and assists the Customs Service in their targeting operations. Known importers who are members of BASC present inherently less risk than unknown non-BASC importers. BASC allows the Customs Service to develop a higher level of confidence that the importer has adequate measures in place to thwart supply chain incursions. The Customs Service is further assured that if there is a successful security breach, that BASC members will report it expeditiously and will cooperate in a resulting investigation to determine the cause of the breach.

During the development of BASC, we learned that in order to design and deploy a meaningful deterrent the entire supply chain, end-to-end, must be examined. During this review it was vital that all key process owners in the supply chain were identified. Stakeholders must be actively engaged to identify and remedy potential vulnerabilities within their realm of responsibility and control.

We also learned that the program must be continually monitored and modified to react to new developments and emerging threats. Adaptable guidelines will also allow Customs to attract a diverse cross section of shippers. There are more than 400,000 importers annually. The top 1,000 importers make up a significant percentage of the total US volume. Instinctively we may be tempted to concentrate enlistment efforts in a new security initiative to America's top tier importer, but it should not be overlooked that the overwhelming majority of the 400,000 importers are small importers without elaborate systems or significant investments in security. Therefore, it is necessary keep the depth and breadth of the entire industry in mind when planning new security initiatives.

Question: What incentives are there for businesses to participate in BASC or other similar private sector initiatives?

By conducting a self-examination and cooperating with Customs to develop a BASC Program, an importer can significantly improve their supply chain security, reducing not only the risk of contamination, but also minimizing theft. BASC participants may also experience fewer cargo examinations, which are costly and time consuming. The Customs Service also contributes in joint training exercises and site reviews.

Traditionally, BASC and other Industry Partnership Programs sponsored by Customs have been strictly voluntary. Any new security initiatives should be designed in similar fashion. The Customs Service should be encouraged to continue developing perks for voluntary participants, although other incentives, such as the creation of a "green lane" at a land border, are restricted by infrastructure.

In my opinion however, an importer's participation in the BASC Program loses visibility inside of Customs because an importer's relationship with the Customs Service is not conducted in a true account-based environment. Customs' ability to work with importers in an account-based atmosphere will not be fully realized until there are adequate systems, reporting and infrastructure at Customs to accommodate this type of management. For example, all Customs ports and/or personnel do not have adequate visibility to Target's cooperation as a member of BASC. Customs' ability to create a true account-based environment is constrained by the antiquated Automated Commercial System (ACS). The Automated Commercial Environment (ACE) now under development is replacing this system. ACE funding has been controversial and difficult to obtain. Customs needs support for the immediate and full funding of ACE and should take any action possible to expedite delivery of this new tool.

Question: Are these technologies effective? Who is purchasing and deploying innovative technologies? Is it the Customs Service? Are private companies utilizing new technologies, and if so, what steps has government taken to work with these industry leaders?

Post September 11th, the development of new technologies used to examine passengers, cargo and conveyances has been very fluid. Customs is presently working with the Department of Defense and the Department of Energy to adapt some existing technology into new inspection tools for the Customs Service.

Currently the most effective and least expensive way to examine cargo is through the use of Non Intrusive Inspections (NII). This technology either detects the presence of contraband by its emissions, or uses energy to examine the article and discern the contents. Current NII equipment used by Customs includes large truck x-rays, vehicle

gamma-ray imaging systems, portable radiation detectors, fiberscopes and vapor/particle detectors. I have also been advised that a device for performing chemical, compound or liquid analysis is in the final stages of development. This apparatus will allow the user to determine if the contents of a shipment have been adulterated. This type of equipment, if unclassified for public consumption, will benefit both Customs and the trade. Other innovative security enhancements, such as placing radiation detectors on port cranes, are being tested with encouraging results.

The Treasury Advisory Group on the Commercial Operations of the Customs Service (COAC) has developed a Technical Advisory Group on Border Security. Within this group is a separate sub-group dedicated to reviewing new and existing technology. This group will then offer recommendations to Treasury on specific technologies that may be applied or modified for use as an inspection tool by the Customs Service. The work of this sub-group has begun and they will make their first report at the January 25, 2002, COAC meeting.

The successful use of technology by the Customs Service will, once again, be limited by the primary system used to drive the new technology. Therefore at the risk of being redundant, continued and complete funding for ACE is imperative. The full build out for ACE is five (5) years. Customs should explore what can be done to accelerate ACE design and development with full funding support from Congress. To the degree possible the ACE architecture must be constructed with maximum elasticity, so as other technology components are invented and deployed, ACE can be readily adapted to interface with the new tools.

Question: What steps can a company such as Target take to develop security in this area?

As with Target Corporation's entry into the BASC Program, new supply chain security initiatives will be captained by the Target Corporation Assets Protection department. Other work groups such as Approved for Purchase, Compliance, Import Transportation, Import Operations, Sourcing, Quality Assurance and Merchandising will be mobilized to augment their efforts.

The international supply chain involves many different stakeholders, so it will be necessary to craft a multi-pronged strategy. I have itemized considerations for each relationship or function below.

Importer/Vendor Relationships

Determining what level of security is currently in place, and what can be done to further improve, is something that should be accomplished at the very onset of a relationship between an importer and foreign vendor. When a vendor is first being evaluated for their

ability to manufacture and deliver a product or material sought by the importer, matters concerning security should be incorporated into that analysis.

For established relationships, security changes need to be communicated by training, on-site surveys and the incorporation of new requirements into the Terms and Conditions language of the contract or purchase order.

Importer/Service Provider Relationships

Local Carriers at Origin: While an internal conspiracy at a factory is not an unlikely scenario, of greater concern is the transportation of the consignment to the terminal or point of departure. Tracking the movement and timing of the cargo is critical and will reveal anomalies that may warrant further investigation to the extent that it is practical. The use of transponders and Global Positioning Satellite (GPS) coordinates are effective in this cause. However, this technology is only being used in a fraction of the origins generating US bound cargo. Furthermore, it is cost prohibitive for many small and medium-sized cartage companies, and in many third world countries. In the absence of GPS tracking, service providers should be encouraged to develop manual alternatives that are capable of recognizing irregularities.

Local privacy or civil liberty laws may restrict background checks for drivers at origin. This notwithstanding, we should beseech foreign governments to consider requiring positive identification for drivers and surety bonds for the company.

Foreign Consolidators and Freight Forwarders: These agents play an important role in the movement of an international consignment. As a consolidator they often accept physical custody of goods being shipped in less than container load quantities. They also perform document collection services, make cargo bookings (reservations), and coordinate the delivery of full container load shipments. As US importers employ the services of these agents, the importer must actively convey their security expectations. Security requirements should be spelled out in any contractual agreement entered into; or at a minimum well documented in the procedures for handling the importer's shipments.

Most freight forwarders operate under licenses granted by the local government or other regulating body. Foreign regulating entities should be persuaded to review all license holders for recent criminal activity. Government sponsored training on how to detect and report suspicious activity should also be offered to the freight forwarding community.

Question: What, if any, channels are in place for a company to give and receive information about suspect suppliers with Customs Service or INS?

Today, to the best of my knowledge, no channels exist between the trade and Customs or the INS to share information about suspect suppliers. A good two-way communication mechanism between the Customs Service and private sector is needed. A periodic exchange of information and certain intelligence with U.S. Customs would be extremely

beneficial. The development of an information repository would give Customs and the trade better visibility. Careful analysis of the inputs into such a database would allow Customs to ascertain new or developing trends. For example, repetitive reports of pilferage in a certain country may be indicative of other criminal activities. Recognition of repetitive incidents may then trigger other investigative and intelligence activities within the Customs Service. It would also prompt Customs to issue a general alert to the trade. The trade community would then utilize these intelligence reports to intensify their security efforts in a certain region. However, we must also be mindful of certain privacy restrictions and the ramifications of accidental implication. Naming an otherwise innocent party as a "high security risk" may have catastrophic results for that entity.

Conclusion

The task of securing foreign cargoes destined for America is daunting. The volumes are intimidating and it is completely impracticable to believe that it is possible to examine 100% of all shipments. Foreign commerce is a major component and engine of our economy. An international supply chain involves many process owners, one size will not fit all and new initiatives should have maximum flexibility. Working in harmony with the private sector, it is necessary for the government to take a leadership role in coordinating the efforts to secure foreign consignments.

Responses to Additional Questions for the Record from
Senator Joseph I. Lieberman
Weak Links: Assessing the Vulnerability of U. S. Ports and Whether the Government is Adequately Structured to Safeguard Them
Hearing Date: December 6, 2001

Submitted by:
W. Gordon Fink
President, Emerging Technology Markets

Question One

A) Are you aware of technologies which map containers according to its elemental composition? How reliable would such a technology be in locating dangerous materials such a weapons or bombs?

Response: I am not aware of technologies that do element composition mapping within a closed container. Most applications rely on the equipment operator to detect the different densities of the materials within the container including the shape of the materials. The operator then uses this information to determine if the container appears to match the manifest or has questionable object shapes or densities. He then relies on a physical inspection of the container to resolve any uncertainty.

B) Are the different technologies better or worse at finding types of illegally imported materials, such as persons, weapons, drugs or bombs?

Response: The SAIC VACIS system uses gamma rays which are considered to be safer that high power x-ray technology especially if people are exposed to the radiation within a container. More testing is needed to help determine the safety of high power x-ray devices including the potential to detonate explosives or to damage contents including electronic devices such as electronic seals.

C) Who is purchasing and deploying innovative technologies? Is it the Customs Service? Are private companies utilizing new technologies, and if so, what steps has government taken to work with these industry leaders?

Response: The U. S. Customs Service originally purchased the VACIS gamma ray systems for use at the U. S. – Mexico land border crossings. Some of these systems may have been redeployed. I understand the Port of Vancouver is purchasing a VACIS system. The U. S. Military has used these systems in Kosovo. The use of these systems is still new and evolving. The private sector is beginning work in image processing software to assist the system operator in detecting questionable content that leads to the decision to pull the container for physical inspection. This would be a good question for the Customs Service especially their future plans for purchase and deployment of this expensive equipment.

D) Companies are concerned about the reduction in efficiency the scanners may cause in through-put. Are there significant differences in through-put rates of scanners which

utilize different technologies? Can the deployment of scanners lead to increased efficiency in the system at other points along the way?

Response: Currently the through-put rates for VACIS (and I presume high power x-ray systems) are up to 10 miles per hour. This is close to the current exit speed for the container truck chassis and rail cars departing the terminals. One terminal operator, who does not have a lot of on-terminal storage space, told me he would consider investing in inspection equipment to insure that his on-terminal cargo flow is not interrupted. There would be a major impact on terminal efficiency if the cargo flow is slowed or stopped because of increased inspection requirements – such as "pulling a container" for inspection on an outbound train. Unless weapons are detected, I understand Customs is considering letting the train proceed and inspecting the suspicious container at its destination.

Question Two

A) What are the advantages of Global Positioning Satellite (GPS) Systems, electronic seals, Smart tags, and security systems which integrate all these systems to insure that the container remains secure on the terminal and during movement to the consignee?

Response: The benefits of these technologies are significant – to U. S. Customs for in-bond shipment monitoring and to the carriers for deterring theft, increasing the efficiency in the use of their assets (chassis, containers, trucks, etc.), and to keep the consignee informed on the estimated cargo delivery time. Systems that integrate many of these technologies are currently in the early stages of deployment. As multiple sources of these systems emerge, the deployment costs will be reduced.

B) Do you believe the use of Smart Cards to be a viable solution to assist in the short term for persons who interact with cargo thus maintaining electronic records for port access and cargo accountability?

Response: The use of Smart Cards could be immediate and add to the security in the storage and movement of cargo – especially if the Smart Cards use some of the recently introduced biometric identifiers such as facial recognition, fingerprints, and/or the iris of the eye to prevent misuse. Unfortunately, the State of Florida is requiring a separate ID for each of their ports by January 1, 2002 causing a major reaction from the dray truck drivers that service several ports and/or terminals. The Port Authority of New York and New Jersey pioneered the use of a common driver ID card (magnetic stripe technology) several years ago for all of their ports and terminals which has deterred theft and added to cargo security. A common, regional or nationwide Smart Card ID (in addition to the commercial drivers license) would be a major short term improvement.

Question Three

What problems are unique to hazardous goods? What role can technology play in safeguarding shipments of hazardous materials or fuels?

Response: I will defer to the Coast Guard with respect to vessels entering ports and terminals. As noted above, Smart Cards (with biometrics) for authorized hazmat vehicle

drivers would be a good first step – especially if the card includes the results of a government conducted criminal background checks. Truck mounted equipment is available that would disable the engine if an unauthorized driver attempts to drive the truck. Truck tracking software is available that would alert the carrier to unauthorized route deviations. Panic or emergency "buttons" can alert carriers/authorities to hijack situations. Carriers are concerned about the potential threats and are currently investigating the use of these technologies.

Question Four

It has been suggested that the United States alone cannot and should not bear the burden for increasing security at ports worldwide. Many smaller nations lack the resources to maintain parity with the increases in security the United States needs to implement. What steps can the private sector take to assist foreign nations to increase security at ports? What incentives are there for foreign nations to invest in advanced technologies?

Response: An easy answer is that the challenge is global and all shippers, ports and carriers should share the costs of improving security. If the private marine carriers (mostly foreign owned) doing business in the U. S. believe they must invest to protect their interests (foreign terminals, vessels, etc.), then they may begin to share in some of the investment costs for increased, worldwide security.

If the shipper starts the security "chain of responsibility" by employing trusted employees to inspect the container and affix the electronic seal, transit ports such as Rotterdam, Hong Kong or Singapore must also invest in the technology to insure the integrity of the container during trans-shipment. In the long term, a non-intrusive image of the container could become a part of the manifest documentation at its origin – to be reviewed prior to the container importation into the U. S. and compared with a second image made at the importing terminal.

A dedicated, worldwide community composed of the public and private sector representatives must draft and implement the new requirements for a global security system and make the decision on how to spread to cost burden – possibly a "per container shipment tax" that would help finance the worldwide investment costs. No one likes the idea of increasing transportation costs but the traveling public, through acceptance of an additional cost to their airfare for additional security, may help set the example for the international freight shipping community. I understand that the Alameda Corridor in Southern California imposes such a "tax" on each container transiting the corridor to help pay off the construction bonds. Mechanisms can be devised to help smaller nations with some of the cost burden but all governments, ports and private carriers must accept the increased cost of doing business to meet the new security requirements for participation in global commerce.

Appendix G

Schedule D

Classification of United States Customs Districts and Ports for U.S. Foreign Trade Statistics. This appendix provides a complete listing of valid district/port codes.

District/Port Codes	
Code	**Port**
	1 Northeast Region
0101	Portland, ME
0102	Bangor, ME
0103	Eastport, ME
0104	Jackman, ME
0105	Vanceboro, ME
0106	Houlton, ME
0107	Fort Fairfield, ME
0108	Van Buren, ME
0109	Madawaska, ME
0110	Fort Kent, ME
0111	Bath, ME
0112	Bar Harbor, ME
0115	Calais, ME
0118	Limestone, ME
0121	Rockland, ME
0122	Jonesport, ME
0127	Bridgewater, ME
0131	Portsmouth, NH
0132	Belfast, ME
0152	Searsport, ME
0181	Lebanon Airport, NH
0201	St. Albans, VT
0203	Richford, VT
0206	Beecher Falls, VT
0207	Burlington, VT
0209	Derby Line, VT
0211	Norton, VT
0212	Highgate Springs/Alburg, VT
0401	Boston, MA
0402	Springfield, MA
0403	Worcester, MA

District/Port Codes	
Code	**Port**
0404	Gloucester, MA
0405	New Bedford, MA
0406	Plymouth, MA
0407	Fall River, MA
0408	Salem, MA
0409	Provincetown, MA
0410	Bridgeport, CT
0411	Hartford, CT
0412	New Haven, CT
0413	New London, CT
0416	Lawrence, MA
0417	Logan Airport, MA
0501	Newport, RI
0502	Providence, RI
0503	Mellville, RI
0701	Ogdensburg, NY
0704	Massena, NY
0705	Fort Covington, NY
0706	Cape Vincent, NY
0708	Alexandria Bay, NY
0711	Chateaugay, NY
0712	Champlain-Rouses Point, NY
0714	Clayton, NY
0715	Trout River, NY
0901	Buffalo-Niagara Falls, NY
0903	Rochester, NY
0904	Oswego, NY
0905	Sodus Point, NY
0906	Syracuse, NY
0907	Utica, NY
0979	Buffalo, NY
1101	Philadelphia, PA
1102	Chester, PA
1103	Wilmington, DE

District/Port Codes	
Code	**Port**
1104	Pittsburgh, PA
1105	Paulsboro, PA
1106	Wilkes-Barre/Scranton, PA
1107	Camden, NJ
1108	Philadelphia Intl. Airport, PA
1109	Harrisburg, PA
1113	Gloucester City, NJ
1118	Marcus Hook, PA
1181	Allentown/Bethlehem/Easton Airport, PA
1301	Annapolis, MD
1302	Cambridge, MD
1303	Baltimore, MD
1304	Crisfield, MD
2 New York Region	
1001	New York, NY
1002	Albany, NY
1003 & 4601	Newark, NJ
1004 & 4602	Perth Amboy, NJ
1069 & 4670	UPS
1070 & 4770	Federal Express, Jamaica, NY
1071 & 4771	NYACC
1072 & 4772	DHL, Jamaica, NY
1081 & 4681	Morristown Airport, Newark, NJ
4701 & 1012	John F. Kennedy Airport, NY
3 North Central Region	
3301	Raymond, MT
3302	Eastport, ID
3303	Salt Lake City, UT
3304	Great Falls, MT
3305	Butte, MT
3306	Turner, MT
3307	Denver, CO
3308	Porthill, ID
3309	Scobey, MT
3310	Sweetgrass, MT
3312	Whitetail, MT
3316	Piegan, MT
3317	Opheim, MT

District/Port Codes	
Code	**Port**
3318	Roosville, MT
3319	Morgan, MT
3321	Whitlash, MT
3322	Del Bonita, MT
3382	Natrona County Intl. Airport, WY
3401	Pembina, ND
3402	Noyes, MN
3403	Portal, ND
3404	Neche, ND
3405	St. John, ND
3406	Northgate, ND
3407	Walhalla, ND
3408	Hannah, ND
3409	Sarles, ND
3410	Ambrose, ND
3413	Antler, ND
3414	Sherwood, ND
3415	Hansboro, ND
3416	Maida, ND
3417	Fortuna, ND
3419	Westhope, ND
3420	Noonan, ND
3421	Carbury, ND
3422	Dunseith, ND
3423	Warroad, MN
3424	Baudette, MN
3425	Pinecreek, MN
3426	Roseau, MN
3481	Hector International Airport, Fargo, ND
3501	Minneapolis-St. Paul, MN
3601	Duluth, MN
3602	Ashland, WI
3604	International Falls/Ranier, MN
3608	Superior, WI
3613	Grand Portage, MN
3614	Silver Bay, MN
3701	Milwaukee, WI
3702	Marinette, WI
3703	Green Bay, WI
3706	Manitowoc, WI
3707	Sheboygan, WI
3708	Racine, WI
3801	Detroit, MI
3802	Port Huron, MI
3803	Sault Ste Marie, MI
3804	Saginaw/Bay City/Flint, MI
3805	Battle Creek, MI

District/Port Codes	
Code	**Port**
3806	Grand Rapids, MI
3808	Escanaba, MI
3809	Marquette, MI
3814	Algonac, MI
3815	Muskegon, MI
3816	Grand Haven, MI
3818	Rogers City, MI
3819	Detour, MI
3820	Mackinac Island, MI
3842	Presque Island, MI
3843	Alpena, MI
3844	Ferrysburg, MI
3881	Oakland/Pontiac Airport, MI
3901	Chicago, IL
3902	Peoria, IL
3903	Omaha, NE
3904	East Chicago, IN
3905	Gary, IN
3906	O'Hare Intl. Airport, IL
3982	Greater Rockford Airport, IL
3991	Nippon Courier Hub, IL
3907	Des Moines, IA
3908	Davenport, IA-Rock Island/Moline, IL
3981	Waukegan Regional Airport, IL
4101	Cleveland, OH
4102	Cincinnati – Lawrenceburg, OH
4103	Columbus, OH
4104	Dayton, OH
4105	Toledo - Sandusky, OH
4106	Erie, PA
4108 & 4122	Ashtabula, OH
4109 & 4122	Conneaut, OH
4110	Indianapolis, IN
4111	Fairport, OH
4112	Akron, OH
4115	Louisville, KY
4116	Owensboro, KY - Evansville, IN
4117	Huron, OH
4121	Lorain, OH
4181	Airborne Air Park, Wilmington, OH
4182	Rickenbacker Airport, Columbus, OH
4183	Fort Wayne Airport, IN
4184	Bluegrass Airport, Lexington, KY
4195	Emery World Wide Courier, Dayton, OH
4196	UPS Courier, Louisville, KY

District/Port Codes	
Code	**Port**
4197	DHL Courier, Cincinnati, OH
4501	Kansas City, MO
4502	St. Joseph, MO
4503	St. Louis, MO
4504	Wichita, KS
4505	Springfield, MO
4 Southeast Region	
1401	Norfolk, VA
1402	Newport News, VA
1404	Richmond-Petersburg, VA
1406	Cape Charles, VA
1407	Reedville, VA
1408	Hopewell, VA
1409	Charleston, WV
1410	Front Royal, VA
1501	Wilmington, NC
1502	Greensboro, NC
1503	Durham, NC
1506	Reidsville, NC
1511	Beaufort-Morehead City, NC
1512	Charlotte, NC
1601	Charleston, SC
1602	Georgetown, SC
1603	Greenville-Spartanburg, SC
1604	Columbia, SC
1701	Brunswick, GA
1703	Savannah, GA
1704	Atlanta, GA
1801	Tampa, FL
1803	Jacksonville, FL
1805	Fernandina Beach, FL
1807	Boca Grande, FL
1808	Orlando, FL
1814	St. Petersburg, FL
1816	Port Canaveral, FL
1818	Panama City, FL
1819	Pensacola, FL
1821	Port Manatee, FL
1881	Southwest Florida Regional Airport, FL
1882	Sanford Regional Airport, FL
4901	Aguadilla, PR
4904	Fajardo, PR
4905	Guanica, PR
4906	Humacao, PR
4907	Mayaguez, PR
4908	Ponce, PR

District/Port Codes	
Code	**Port**
4909	San Juan, PR
4911	Jobos, PR
4912	Guayanilla, PR
4913	San Juan Intl. Airport, PR
5101	Charlotte Amalie, Virgin Islands
5102	Cruz Bay, Virgin Islands
5103	Coral Bay, Virgin Islands
5104	Christiansted, Virgin Islands
5105	Frederiksted, Virgin Islands
5201	Miami, FL
5202	Key West, FL
5203	Port Everglades, FL
5204	West Palm Beach, FL
5205	Fort Pierce, FL
5206	Miami Intl. Airport , Miami, FL
5270	International Courier Association
5401	Washington, DC
5402	Alexandria, VA
5 South Central Region	
1901	Mobile, AL
1902	Gulfport, MS
1903	Pascagoula, MS
1904	Birmingham, AL
1910	Huntsville, AL
2001	Morgan City, LA
2002	New Orleans, LA
2003	Little Rock/North Little Rock, AR
2004	Baton Rouge, LA
2005	Port Sulphur, LA
2006	Memphis, TN
2007	Nashville, TN
2008	Chattanooga, TN
2009	Destrehan, LA
2010	Gramercy, LA
2011	Greenville, MS
2012	Avondale, LA
2013	St. Rose, LA
2014	Good Hope, LA
2015	Vicksburg, MS
2016	Knoxville, TN
2017	Lake Charles, LA
2018	Shreveport-Bossier City, LA
2095	Federal Express Courier, Memphis, TN
2101	Port Arthur, TX
2102	Sabine, TX

District/Port Codes	
Code	**Port**
2103	Orange, TX
2104	Beaumont, TX
6 Southwest Region	
2301	Brownsville-Cameron County, TX
2302	Del Rio, TX
2303	Eagle Pass, TX
2304	Laredo, TX
2305	Hidalgo, TX
2307	Rio Grande City, TX
2309	Progresso, TX
2310	Roma, TX
2402	El Paso, TX
2403	Presidio, TX
2404	Fabens, TX
2406	Columbus, NM
2407	Albuquerque, NM
2481	Santa Teresa Airport, Dona Ana County, NM
2601	Douglas, AZ
2602	Lukeville, AZ
2603	Naco, AZ
2604	Nogales, AZ
2605	PhoenixAZ
2606	Sasabe, AZ
2608	San Luis, AZ
2609	Tucson, AZ
5301	Houston, TX
5306	Texas City, TX
5309	Houston Intercontinental Airport, Houston,TX
5310	Galveston, TX
5311	Freeport, TX
5312	Corpus Christi, TX
5313	Port Lavaca, TX
5501	Dallas/Ft. Worth Airport, TX
5502	Amarillo, TX
5503	Lubbock, TX
5504	Oklahoma City, OK
5505	Tulsa, OK
5506	Austin, TX
5507	San Antonio, TX
5582	Midland International Airport, TX
7 Pacific Region	
2501	San Diego, CA
2502	Andrade, CA
2503	Calexico, CA
2504	San Ysidro, CA
2505	Tecate, CA

District/Port Codes	
Code	**Port**
2506	Otay Mesa Station, CA
2704	Los Angeles, CA
2707	Port San Luis, CA
2709	Long Beach, CA
2711	El Segundo, CA
2712	Ventura, CA
2713	Port Hueneme, CA
2715	Capitan, CA
2719	Morro, CA
2720	Los Angeles Intl. Airport, Los Angeles, CA
2722	Las Vegas, NV
2770	DHL Worldwide, Los Angeles, CA
2772	Gateway Freight Services, LAX
2773	Air Cargo Handling Services, Inc.
2795	UPS, Ontario, CA
2801	San Francisco Intl. Airport,San Francisco, CA
2802	Eureka, CA
2803	Fresno, CA
2805	Monterey, CA
2809	San Francisco, CA
2810	Stockton, CA
2811	Oakland, CA
2812	Richmond, CA
2813	Alameda, CA
2815	Crockett, CA
2816	Sacramento, CA
2820	Martinez, CA
2821	Redwood City, CA
2827	Selby, CA
2828	San Joaquin River, CA
2829	San Pablo Bay, CA
2830	Carquinez Strait, CA
2831	Suisun Bay, CA
2833	Reno, NV
2834	San Jose International, San Francisco, CA
2870	DHL Worldwide Express, San Francisco, CA
2871	Air Cargo Handling Services, San Francisco, CA
2901	Astoria, OR
2902	Newport, OR
2903	Coos Bay, OR
2904	Portland, OR
2905	Longview, WA
2907	Boise, ID
2908	Vancouver, WA
2909	Kalama, WA
2981	Kingsley Field, Klamath Falls, OR

District/Port Codes	
Code	**Port**
2991	Federal Express Courier, Portland, OR
3001	Seattle, WA
3002	Tacoma, WA
3003	Aberdeen/Hoquiam, WA
3004	Blaine, WA
3005	Bellingham, WA
3006	Everett, WA
3007	Port Angeles, WA
3008	Port Townsend, WA
3009	Sumas, WA
3010	Anacortes, WA
3011	Nighthawk, WA
3012	Danville, WA
3013	Ferry, WA
3014	Friday Harbor, WA
3015	Boundary, WA
3016	Laurier, WA
3017	Point Roberts, WA
3018	Kenmore Air Harbor, WA
3019	Oroville, WA
3020	Frontier, WA
3022	Spokane, WA
3023	Lynden, WA
3025	Metaline Falls, WA
3026	Olympia, WA
3027	Neah Bay, WA
3029	Seattle-Tacoma Intl. Airport, WA
3081	Yakima Air Terminal, Yakima, WA
3101	Juneau, AK
3102	Ketchikan, AK
3103	Skagway, AK
3104	Alcan, AK
3105	Wrangell, AK
3106	Dalton Cache, AK
3107	Valdez, AK
3111	Fairbanks, AK
3112	Petersburg, AK
3115	Sitka, AK
3124	Pelican, AK
3125	Sand Point, AK
3126	Anchorage, AK
3127	Kodiak, AK
3181	Saint Paul Airport, Anchorage, AK
3195	Federal Express, Anchorage, AK
3196	UPS, Anchorage, AK
3201	Honolulu, HI
3202	Hilo, HI

District/Port Codes	
Code	**Port**
3203	Kahului, HI
3204	Nawiliwili-Port Allen, HI
3205	Honolulu Intl. Airport, HI
3295	UPS, Honolulu Airport, HI